A comparison of refinement orderings and their associated simulation rules

Christie Bolton, Jim Davies\textsuperscript{1,2}

\textit{Oxford University Computing Laboratory}
\textit{Wolfson Building, Parks Road}
\textit{Oxford OX1 3QD, England}

\begin{abstract}
In this paper we compare the refinement orderings, and their associated simulation rules, of state-based specification languages such as Z and Object-Z with the refinement orderings of event-based specification languages such as CSP. We prove with a simple counter-example that data refinement, established using the standard simulation rules for Z, does not imply failures refinement in CSP. This contradicts accepted results.

Having explored the differences between the simulation rules for establishing data refinement and those for establishing the refinement of action systems and state-transition systems—models in which refinement is equivalent to failures refinement within CSP—we present a new set of simulation rules for data types. These alternative rules are both sound and jointly complete with respect to the stable failures refinement ordering. Furthermore we present an alternative refinement ordering for CSP, one in which refinement is equivalent to data refinement in Z.
\end{abstract}

\section{Introduction}
During the development of large complex systems it is often desirable to construct a series of models, each model resolving ambiguities or areas of undefinedness in the previous model. In such a methodology we may wish to prove formally that each model is refined by the next. Our intuition tells us that one model is refined by another if the second model satisfies all the properties and constraints imposed by the first. As we will illustrate, the precise definition of refinement depends on our chosen formalism.

In this paper we focus on the refinement of abstract data types expressed in the state-based specification languages Z \cite{22} and Object-Z \cite{10}, and the

\begin{itemize}
\item \textsuperscript{1} Email: christie@comlab.ox.ac.uk
\item \textsuperscript{2} Email: jdavies@comlab.ox.ac.uk
\end{itemize}

\copyright 2002 Published by Elsevier Science B. V. Open access under CC BY-NC-ND license.
refinement of processes expressed in the event-based specification language CSP [13]. Refinement within both Z and Object-Z generally employs sets of simulation rules [14], although it may be established by considering the relational semantics within Z or by considering the histories semantics [19] within Object-Z.

We expose and discuss the differences between data refinement [8] and refinement within the stable failures model [18] for CSP, and we show that whilst both models give information about possible sequences of interaction and both models give refusal information, they are not equivalent. The stable failures and failures-divergences [18] models within CSP give information about the availability of combinations of events whereas the relational semantics of Z gives refusal information only about individual operations. Hence, data refinement does not imply failures refinement.

In Section 2 we present a simple counter-example proving that the simulation rules derived to correspond precisely to the blocking interpretation of the relational semantics [5] of data types expressed in Z are not sound with respect to the stable failures model [18] of CSP. From this it follows immediately that data refinement does not imply stable failures refinement, contradicting accepted results [21,6,5,11,9].

Having explored the differences between these two refinement orderings, we have two options if we wish to compare state-based and event-based models: either we must identify a semantic model for CSP that has the same information content as the relational semantics of data types, or we must identify a set of simulation rules that correspond to the stable failures model for CSP. We adopt the former approach in Section 5 and, having explored the differences between the simulation rules for establishing data refinement and those for establishing the refinement of action systems [1] and state-transition systems [17,16]—models in which refinement is equivalent to failures refinement within CSP—in Section 3, we adopt the latter approach in Section 4. The main contributions of the paper are as follows:

- we demonstrate that data refinement in Z does not imply stable failures refinement within CSP;
- we present a set of simulation rules for data types expressed in Object-Z that are both sound and jointly complete with respect to the stable failures refinement ordering of CSP;
- we describe an alternative semantic model for CSP whose information content is precisely that of the relational semantics of data types;

---

3 As illustrated in [4] this results extends to Object-Z.
4 In this paper we assume knowledge of Z, Object-Z and CSP. Readers unfamiliar with these notations should see [22,23,9], and [20] and [13,18] respectively.
5 Object-Z rather than Z is our chosen paradigm as, for divergence-free systems, these simulation rules correspond precisely to the established histories model for Object-Z.
2 Data refinement does not imply failures refinement

We prove that data refinement is not equivalent to stable failures refinement with a simple example as described in [2]. Let data types $P$ and $Q$ be defined as follows: both data types have the same internal state space $State$ containing the integers from 0 up to 4; given environment $Env$ containing the single element $e$, both data types have the same finalisation operations mapping the entire state space onto $Env$;

\[
\begin{array}{c}
\text{State} \\
\text{s : 0 . . 4}
\end{array}
\quad
\begin{array}{c}
\text{Final} \\
\text{State; Env'}
\end{array}
\]

and both data types share the operations $A$, $B$ and $C$ as illustrated in Figure 1. Operation $A$ maps state 1 onto state 0; operation $B$ maps states 2 and 3 onto state 0; and operation $C$ maps states 2 and 4 onto state 0. More formally,

\[
\begin{array}{c}
\text{A} \\
\text{\Delta State} \\
\text{s = 1 \land s' = 0}
\end{array}
\quad
\begin{array}{c}
\text{B} \\
\text{\Delta State} \\
\text{s \in \{2, 3\} \land s' = 0}
\end{array}
\quad
\begin{array}{c}
\text{C} \\
\text{\Delta State} \\
\text{s \in \{2, 4\} \land s' = 0}
\end{array}
\]

The difference between the two data types lies in the range of their initialisation relations: data type $P$ can initially be in states 1 or 2 whereas data type $Q$ can initially be in states 1, 3 or 4.
Fig. 2. The backwards relation Retr from State\(_Q\) to State\(_P\).

Weprovein Lemma 2.1 below that datatypetype \(P\) is refined by datatypetype \(Q\) by proving that \(P\) simulates \(Q\) within the context of the blocking semantics\(^6\); more specifically we identify a retrieverelation Retr such that the backwards simulation rules corresponding to the blocking semantics, as presented in Appendix A, all hold. Data refinement follows automatically due to the soundness of the simulation rules [5].

**Lemma 2.1** Data type \(P\) is refined by \(Q\) where \(P\) and \(Q\) are as defined above.

**Proof.** For clarity, we distinguish syntactically between the shared components of the data types; we define \(\text{State}_P\) and \(\text{State}_Q\) to be equal to \(\text{State}\); \(A_P\) and \(A_Q\) to be equal to \(A\) and so on. Then letting retrieverelation Retr from the state space of \(Q\) to the state space of \(P\) be as illustrated in Figure 2 and formally defined below:

\[
\begin{array}{c|c}
\text{PInit} & \text{QInit} \\
\hline
\text{Env; State} & \text{Env; State} \\
\hline
s^\prime \in \{1, 2\} & s^\prime \in \{1, 3, 4\}
\end{array}
\]

we simply need to prove that the following predicates are true.

(i) \(\forall \text{State}_P^\prime; \text{State}_Q^\prime \cdot \text{QInit} \land \text{Retr}^\prime \Rightarrow \text{PInit}\)

(ii) (a) \(\forall \text{State}_Q \cdot (\forall \text{State}_P \cdot \text{Retr} \Rightarrow \text{pre } A_P) \Rightarrow \text{pre } A_Q\)

(b) \(\forall \text{State}_Q \cdot (\forall \text{State}_P \cdot \text{Retr} \Rightarrow \text{pre } B_P) \Rightarrow \text{pre } B_Q\)

(c) \(\forall \text{State}_Q \cdot (\forall \text{State}_P \cdot \text{Retr} \Rightarrow \text{pre } C_P) \Rightarrow \text{pre } C_Q\)

(iii) (a) \(\forall \text{State}_P^\prime; \text{State}_Q^\prime \cdot A_Q \land \text{Retr}^\prime \cdot (\exists \text{State}_P \cdot \text{Retr} \land A_P)\)

\(^6\) We work within the blocking framework to facilitate our comparison in Section 3.
(b) \( \forall \text{State}_P; \text{State}_Q; \text{State}'_Q \mid B_Q \land \text{Retr}' \bullet (\exists \text{State}_P \bullet \text{Retr} \land B_P) \)

(c) \( \forall \text{State}_P; \text{State}_Q; \text{State}'_Q \mid C_Q \land \text{Retr}' \bullet (\exists \text{State}_P \bullet \text{Retr} \land C_P) \)

(iv) \( \forall \text{State}_Q; \text{Env} \mid \text{Final}_Q \bullet \exists \text{State}_P \mid \text{Retr} \bullet \text{Final}_P \)

The first rule reduces to

\[
\forall p', q' : \text{State} \bullet \left( ((q' = 1 \land p' = 1) \lor ((q' = 3 \lor q' = 4) \land (p' = 1 \lor p' = 2))) \Rightarrow (p' = 1 \lor p' = 2) \right)
\]

which is equivalent to true. In the case of operation \(A\), the inner clause of the second rule, or to be precise the predicate \(\forall \text{State}_P \bullet \text{Retr} \Rightarrow \text{pre}_A P\), is equivalent to

\[
\forall p : \text{State} \bullet \left( (q = 0 \land p = 0) \lor (q = 1 \land p = 1) \lor (q = 2 \land p = 2) \lor (q = 3 \land (p = 1 \lor p = 2)) \lor (q = 4 \land (p = 1 \lor p = 2)) \right) \Rightarrow p = 1
\]

which reduces to \(q \neq 0 \land q \neq 2 \land q \neq 3 \land q \neq 4\) and hence to \(q = 1\). In the case of operation \(A\), the second rule is therefore equivalent to

\[
\forall q : \text{State} \bullet q = 1 \Rightarrow q = 1
\]

which is of course true. Similarly, in the case of operation \(B\), the inner clause of the second rule is equivalent to

\[
\forall p : \text{State} \bullet \left( (q = 0 \land p = 0) \lor (q = 1 \land p = 1) \lor (q = 2 \land p = 2) \lor (q = 3 \land (p = 1 \lor p = 2)) \lor (q = 4 \land (p = 1 \lor p = 2)) \right) \Rightarrow (p = 2 \lor p = 3)
\]

which reduces to \(q \neq 0 \land q \neq 1 \land q \neq 3 \land q \neq 4\) and hence to \(q = 2\). In the case of operation \(B\), the second rule is therefore equivalent to

\[
\forall q : \text{State} \bullet q = 2 \Rightarrow ((q = 2) \lor (q = 3))
\]

which is once again true. Furthermore, by symmetry it follows immediately that the second rule must also be true for operation \(C\).
We have shown that rule one holds and that rules two holds for each of the operations on the data types. Next we consider the third rule. In the case of operation $A$ this rule reduces to

$$\forall p', q, q' : State \mid q = 1 \land q' = 0 \land p' = 0 \bullet$$

$$\exists p : State \bullet p = 1 \land p' = 0 \land (q = 1 \lor q = 3 \lor q = 4)$$

which is equivalent to true. In the case of operation $B$, the third rule reduces to

$$\forall p', q, q' : State \mid (q = 2 \lor q = 3) \land q' = 0 \land p' = 0 \bullet$$

$$\exists p : State \bullet p = 2 \land p' = 0 \land (q = 2 \lor q = 3 \lor q = 4)$$

$$\lor p = 3 \land p' = 0 \land false$$

which is also equivalent to true. Once more we appeal to symmetry to establish immediately that the third rule must also be true for operation $c$.

Finally, observing that the fourth simulation rule is trivially true, we conclude that all the backwards simulation rules hold and hence that $P$ simulates $Q$. Hence, by the soundness of the simulation rules [5], we deduce that data type $P$ is refined by data type $Q$. □

Applying the natural translation from data types within a blocking context to CSP processes (see: [24] for further details) we obtain $\text{process}_b(P)$, the process corresponding to data type $P$.

$$\text{process}_b(P) = \text{let}$$

$$P(s) = (s == 0) \& \text{Stop}$$

$$\text{within}$$

$$\text{init.e} \rightarrow P(s)$$
With a little rearranging and some obvious renaming, this process may equivalently be written as process $\text{ProcP}$ below:

$$
\text{ProcP} = i \rightarrow ( ( a \rightarrow f \rightarrow \text{Stop} \\
\square \hfill ( b \rightarrow f \rightarrow \text{Stop} ) \square ( c \rightarrow f \rightarrow \text{Stop} ) ) \\
\square \hfill f \rightarrow \text{Stop} )
$$

Applying similar techniques we may obtain the process $\text{ProcQ}$ corresponding to data type $Q$.

$$
\text{ProcQ} = i \rightarrow ( ( a \rightarrow f \rightarrow \text{Stop} \\
\square \hfill b \rightarrow f \rightarrow \text{Stop} \\
\square \hfill c \rightarrow f \rightarrow \text{Stop} ) \\
\square \hfill f \rightarrow \text{Stop} )
$$

**Observation 1** The process corresponding to $P$ is not refined within the stable failures model by the process corresponding to $Q$ where data types $P$ and $Q$ are as defined above.

**Proof.** We see that after event $i$, the process $\text{ProcP}$ can refuse any set of events that does not contain $f$ and that does not contain both $a$ and $b$, or both $a$ and $c$, whereas, after event $i$ the process $\text{ProcQ}$ can refuse any set of events that does not contain $f$ and that contains at most two of $a$, $b$ and $c$. In particular, $\text{ProcQ}$ can refuse the sets $\{a, b\}$ and $\{a, c\}$ whereas $\text{ProcP}$ cannot: the trace-refusal pairs $(\langle i \rangle, \{a, b\})$ and $(\langle i \rangle, \{a, c\})$ both lie in the failures of $\text{ProcQ}$ but not of $\text{ProcP}$.

We have shown that the set of failures of the process corresponding to $Q$ is not a subset of the set of failures of the process corresponding to $P$. Hence the process corresponding to $P$ is not refined within the stable failures model by the process corresponding to $Q$.

**Theorem 2.2** Data refinement does not imply stable failures refinement

**Proof.** We have identified two data types $P$ and $Q$. In Lemma 2.1 we proved that $P$ is refined by $Q$ and in Observation 1 we proved that the process corresponding to $P$ is not refined within the stable failures semantic model by the process corresponding to $Q$. From this it follows that data refinement does not imply stable failures refinement: data refinement and stable failures refinement are not equivalent. We proved this result within the context of the blocking semantics. A similar proof could be shown to establish the same result in the context of the non-blocking semantics.

\[\square\]
3 The simulation rules of Josephs, He, Woocock and Morgan

Simulation rules for abstract data types expressed in Z may be given either in terms of the schemas defining the components—state space, initialisation, finalisation and named operations—of the data types, or in terms of the underlying relations. Furthermore simulation rules may be derived to correspond to either a blocking or a non-blocking semantic model (see [6]). Whichever context we choose, two sets of simulation rules, forwards and backwards (sometimes referred to as downwards and upwards), will be presented. If some of the non-determinism has been resolved then we look to establish a forwards simulation, whereas if some of the non-determinism of the more abstract of the two data types has been postponed then we look to establish a backwards simulation. The non-blocking and blocking versions of the simulation rules are shown to be sound and jointly complete in [23] and [5] respectively.

In this section we compare the information content of simulation rules for establishing data refinement within Z to the simulation rules of Josephs [15], He [12], and Woocock and Morgan [25]. Woodcock and Morgan’s simulation rules are for establishing the refinement of action systems and He and Josephs rules are for establishing the refinement of state transition systems⁷. These models each adopt a blocking approach, hence our choice of context in Section 2.

Josephs, He, and Woocock and Morgan have each proved that their simulation rules are sound and jointly complete with respect to Roscoe’s failures-divergences refinement ordering; it follows that, for divergence-free systems, they are sound and jointly complete with respect to his stable failures refinement ordering. Syntax aside, the difference between these rules and those corresponding to the data refinement in Z is that the rules of Josephs, He, and Woocock and Morgan each capture the availability of combinations of operations whereas the simulation rules derived from the relational semantics of Z provide information only about the availability of individual operations. This discrepancy occurs only in one rule, the backwards simulation rule concerning the availability of operations. The relevant rules of Josephs, He, and Woocock and Morgan ensures that if a state within the more concrete model lies outside the preconditions (union of the domains) of any given set of actions or transitions, then there must be a corresponding state within the more abstract model that also lies outside the preconditions of that set of operations. The corresponding rule for data types is weaker: it requires that if a state within the more concrete model lies outside the domain of an individual operation then there must be a corresponding state within the more abstract model that also lies outside the domain of that individual operation.

Consider once more data types P and Q as presented in Section 2. State

---

⁷ We assume knowledge of the action systems formalism and of state transition systems. Readers unfamiliar with these notations should see [7].
3 on data type $Q$ lies outside the domains of both operations $A$ and $C$. We identified corresponding state 2 on data type $P$ which lies outside the domain of operation $A$ as well as corresponding state 1 on $P$ which lies outside the domain of $C$; hence the third backwards simulation rule held. However, had we been required to identify a single corresponding state lying outside the domain of both these operations, we would have failed: there is no such corresponding state. Had we translated $P$ and $Q$ to the appropriate formalisms, the simulation rules of Josephs, He, and Woodcock and Morgan would not have held.

4 Simulation rules corresponding to the histories semantic model for Object-Z

In this section we present rules for verifying that one data type is refined by another within the stable failures model. We do this in the context of Object-Z [10] since that has traditionally been given a histories semantics that is equivalent to Roscoe’s failures-divergences semantic model [19]. These rules were introduced in [2,4].

If $A$ and $C$ are Object-Z classes with the same set of operation names $X$, then given a retrieve relation $Retr$ relating the state spaces of the two classes, the forwards/downwards and backwards/upwards simulation rules corresponding to the histories semantic model are respectively as follows.

$$\forall C.\text{STATE} \bullet C.\text{INIT} \Rightarrow (\exists A.\text{STATE} \bullet A.\text{INIT} \land Retr) \quad (\text{FOZ-h} \ 1)$$

$$\forall Op : X; A.\text{STATE}; C.\text{STATE} \bullet \quad (\text{FOZ-h} \ 2)$$

$$Retr \Rightarrow (\text{pre } A.\text{OP} \Leftrightarrow \text{pre } C.\text{OP})$$

$$\forall Op : X; A.\text{STATE}; C.\text{STATE}; C.\text{STATE}' \bullet \quad (\text{FOZ-h} \ 3)$$

$$Retr \land C.\text{OP} \Rightarrow \exists A.\text{STATE}' \bullet Retr' \land A.\text{OP}$$

$$\forall A.\text{STATE}; C.\text{STATE} \bullet C.\text{INIT} \land Retr \Rightarrow A.\text{INIT} \quad (\text{BOZ-h} \ 1)$$

$$\forall C.\text{STATE} \bullet \exists A.\text{STATE} \bullet \quad (\text{BOZ-h} \ 2)$$

$$\forall Op : X \bullet Retr \land (\text{pre } A.\text{OP} \Rightarrow \text{pre } C.\text{OP})$$

$$\forall Op : X; A.\text{STATE}'; C.\text{STATE}; C.\text{STATE}' \bullet \quad (\text{BOZ-h} \ 3)$$

$$Retr' \land C.\text{OP} \Rightarrow \exists A.\text{STATE} \bullet Retr \land A.\text{OP}$$

The soundness and join completeness of these rules follows directly from the corresponding result for Josephs’ rules [4]. They differ from the stan-
dard [9] simulation rules for Object-Z as described in Appendix B only in the rule $B\cdot 2$. The difference lies in the scope of the quantifications: in rule $B_{OZ-r} \cdot 2$ we have the universal quantification of all operations over the existential quantification of all abstract states ($\forall Op : X \bullet \exists A.State \bullet \ldots$) whereas in rule $B_{OZ-h} \cdot 2$ we have a stronger predicate, the existential quantification of all abstract states over the universal quantification of all operations ($\exists A.State \bullet \forall Op : X \bullet \ldots$).

5 The singleton failures semantic model

Having identified the discrepancy between data refinement and stable failures refinement, and having identified simulation rules for Object-Z that are both sound and jointly complete with respect to Roscoe’s failures divergences refinement ordering, we now present a simplified version of the singleton failures semantic model for CSP - a model defined such that its information content is precisely that of the relational semantics of data types. This model was introduced, and shown to be equivalent to the relational semantics of data types in [3,2].

The singleton failures semantic model, mirroring the information content of the relational semantics of data types, records availability of events on an individual basis. The semantic function is essentially\(^8\) a projection of the stable failures semantic function, recording only those trace-refusal pairs in which the cardinality of the refusal set is at most one. Given the set $\text{Refusal}_1$ containing sets of events of cardinality at most one, and the set $\text{Trace}$ containing all possible sequences of events, the simplified version of the semantic function $S$ is defined as follows:

$$S[P] = F[P] \cap (\text{Trace} \times \text{Refusal}_1).$$

where $P$ is a basic process, that is a process constructed using only the operators $\text{Stop}$, $\rightarrow$, $\cap$, $\square$, and $x \parallel y$.

As with the other models within CSP, refinement is reverse containment. Given any basic processes $P$ and $Q$,

$$P \sqsubseteq S Q \iff S[Q] \subseteq S[P].$$

Furthermore, all laws that hold for the stable failures model and that are expressible only in terms of the basic operators hold for the singleton failures model when applied to basic processes.

\(^8\) The exception is the hiding operator with which, for simplicity, we will not concern ourselves in this paper. The interested reader should see [3,2].
6 Conclusions

The new ideas contained within this paper all stem from the observation that data refinement is not equivalent to stable failures refinement. We presented a simple example that exposed the discrepancy between the models: the relational semantics of data types records the availability of operations individually whereas the stable failures semantic model records the availability of combinations of events.

If we wish to compare state-based and event-based models, either we must adopt a set of simulation rules that are both sound and jointly complete with respect to stable failures or failures-divergences models (we took this approach in Section 4, presenting such a set of rules for Object-Z), or we must adopt a semantic model for CSP that has the same information content as the relational semantics of data types (we took this approach in Section 5, introducing the singleton failures semantic model).

We conclude the paper with a table that provides a comparison between the information content of the refinement orderings and simulation rules that we have considered in this paper. We split them into two categories: those that provide refusal information on an individual basis, and those that provide refusal information for combinations of events or operations.

| Individual refusal information | Refinement model | Simulation rules |
|-------------------------------|------------------|-----------------|
| Data refinement eg [8]        | Z eg [23,5,9]    |
| Data refinement in Z eg [23,5,9] | Object-Z eg [21,9] |
| Singleton failures model for CSP eg [3,2] | |

| Combined refusal information | Refinement model | Simulation rules |
|------------------------------|------------------|-----------------|
| Stable failures model for CSP eg [18] | State transition systems eg [15,12] |
| Histories model for Object-Z eg [19] | Action systems eg [25] |
| Concurrent rules for Object-Z eg [4] | |
A Simulation rules for Z

In this section we present the simulation rules for Z within the context of the blocking semantic model\(^9\). Given data types A and C with state spaces \(AState\) and \(CState\), with initialisations and finalisations \(AInit\) and \(AFinal\), and \(CInit\) and \(CFinal\) respectively and with corresponding operations \(AOp\) and \(COp\), and given retrieve relation \(Retr\), the schema versions of the blocking forwards simulation rules are:

\[
\forall CState' \bullet CInit \Rightarrow \exists AState' \mid AInit \bullet Retr \\
(F_Z \, 1)
\]

\[
\forall AState \mid \text{pre} \ AOp \bullet \forall CState \mid \text{pre} \ COp \bullet Retr \\
(F_Z \, 2)
\]

\[
\forall AState \bullet \forall CState \mid \text{pre} \ Retr \\
(F_Z \, 3)
\]

\[
\forall AState \bullet \forall CState \mid \text{pre} \ Retr' \\
\] (F_Z 4)

Similarly, the schema versions of the blocking backwards simulation rules are as follows.

\[
\forall AState'; \ CState' \bullet CInit \land Retr' \Rightarrow AInit \\
(B_Z \, 1)
\]

\[
\forall CState \bullet (\forall AState \bullet Retr \Rightarrow \text{pre} \ AOp) \Rightarrow \text{pre} \ COp \\
(B_Z \, 2)
\]

\[
\forall AState'; \ CState; \ CState' \mid \text{COp} \land Retr' \bullet \\
(B_Z \, 3)
\]

\[
\exists AState \bullet Retr \land AOp \\
\]

\[
\forall CState; \ Env \mid \text{CFinal} \bullet \exists AState \mid Retr \bullet AFinal \\
(B_Z \, 4)
\]

B Simulation rules for Object-Z

In this section we present the simulation rules for Object-Z. These rules are sound and jointly complete with respect to the relational semantics given to Object-Z: see [9]. If \(A\) and \(C\) are Object-Z classes with the same set of operation names \(X\), then given a retrieve relation \(Retr\) relating the state spaces of the two classes, the forwards/downwards and backwards/upwards

\(^9\) For a more detailed description of this model and the derivation of the simulation rules, see [5,2].
Simulation rules for Object-Z, as presented in [21,9], are respectively as follows:

\[ \forall C.\text{STATE} \bullet C.\text{INIT} \Rightarrow (\exists A.\text{STATE} \bullet A.\text{INIT} \land \text{Retr}) \]  
\( \text{(F}_{\text{OZ-r}} \, 1) \)

\[ \forall \text{OP} : X; A.\text{STATE}; C.\text{STATE} \bullet \]  
\[ \text{Retr} \Rightarrow (\text{pre A.}\text{OP} \leftrightarrow \text{pre C.}\text{OP}) \]  
\( \text{(F}_{\text{OZ-r}} \, 2) \)

\[ \forall \text{OP} : X; A.\text{STATE}; C.\text{STATE} \bullet (C.\text{STATE}') \bullet \]  
\[ \text{Retr} \land C.\text{OP} \Rightarrow (\exists A.\text{STATE}' \bullet \text{Retr}' \land A.\text{OP}) \]  
\( \text{(F}_{\text{OZ-r}} \, 3) \)

\[ \forall A.\text{STATE}; C.\text{STATE} \bullet C.\text{INIT} \land \text{Retr} \Rightarrow A.\text{INIT} \]  
\( \text{(B}_{\text{OZ-r}} \, 1) \)

\[ \forall \text{OP} : X; C.\text{STATE} \bullet \]  
\[ \exists A.\text{STATE} \bullet \text{Retr} \land (\text{pre A.}\text{OP} \Rightarrow \text{pre C.}\text{OP}) \]  
\( \text{(B}_{\text{OZ-r}} \, 2) \)

\[ \forall \text{OP} : X; A.\text{STATE}'; C.\text{STATE}; C.\text{STATE}' \bullet (C.\text{STATE}') \bullet \]  
\[ \text{Retr}' \land C.\text{OP} \Rightarrow (\exists A.\text{STATE} \bullet \text{Retr} \land A.\text{OP}) \]  
\( \text{(B}_{\text{OZ-r}} \, 3) \)

References

[1] R. J. R. Back and R. Kurki-Suonio. Decentralisation of process nets with centralised control. In *In 2nd ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, 1983.

[2] C. Bolton. *On the refinement of state-based and event-based models*. PhD thesis, University of Oxford, January 2002. Submitted for examination.

[3] C. Bolton and J. Davies. A singleton failures semantics for communicating sequential processes, 2001. Submitted to Formal Aspects of Computing.

[4] C. Bolton and J. Davies. Refinement in object-z and csp. In M. Butler, K. Sere, and L. Petre, editors, *Proceedings of Integrated Formal Methods (IFM’02)*, Lecture Notes in Computer Science. Springer Verlag, 2002. To appear.

[5] C. Bolton, J. Davies, and J. Woodcock. On the refinement and simulation of data types and processes. In K. Araki, A. Galloway, and K. Taguchi, editors, *Proceedings of Integrated Formal Methods (IFM’99)*. Springer, 1999.

[6] H. Bowman and J. Derrick. A junction between state-based and behavioural specification. In A. Fantechi P. Ciancarini and R. Gorrieri, editors, *Proceedings of Formal Methods for Open Object-Based Distributed Systems (FMOODS ’99)*. Kluwer, 1999.

[7] M. J. Butler. *A CSP approach to action systems*. PhD thesis, University of Oxford, 1992.
[8] W.-P. de Roever and K. Engelhardt. Data Refinement: Model-oriented Proof Methods and their Comparison. Cambridge Tracts in Theoretical Computer Science, 1998.

[9] J. Derrick and E. Boiten. Refinement in Z and Object-Z. Springer, 2001.

[10] R. Duke, G. Rose, and G. Smith. Object-Z: a specification language advocated for the description of standards. Computer Standards and Interfaces, 17, 1995.

[11] C. Fischer. Combination and implementation of processes and data: from CSP-OZ to Java. PhD thesis, University of Oldenburg, 2000.

[12] J. He. Process refinement. In J. McDermid, editor, The theory and practice of refinement. Butterworths, 1989.

[13] C. A. R. Hoare. Communicating Sequential Processes. Prentice Hall, 1985.

[14] C. A. R. Hoare, J. He, and J. W. Sanders. Prespecification in data refinement. Information Processing Letters, 1987.

[15] M. B. Josephs. A state-based approach to communicating processes. Distributed Computing, 3:9–18, 1988.

[16] L. Lamport. A simple approach to specifying concurrent systems. Communications of the ACM, 32(1), 1989.

[17] A. Pnueli. Specification and development of reactive systems. In H.-J. Kugler, editor, Proceedings of (), IFIP, North Holland, 1986. Information Processing.

[18] A. W. Roscoe. The Theory and Practice of Concurrency. Prentice Hall Series in Computer Science, 1998.

[19] G. Smith. A fully abstract semantics of classes for Object-Z. Formal Aspects of Computing, 7, 1995.

[20] G. Smith. The Object-Z specification language. Kluwer Academic Publishers, 2000.

[21] G. Smith and J. Derrick. Refinement and verification of concurrent systems specified in Object-Z and CSP. In M. Hinchey and Shaoying Liu, editors, Proceedings of First IEEE International Conference on Formal Engineering Methods (ICFEM ’97). IEEE Computer Society, 1997.

[22] J. M. Spivey. The Z notation: a reference manual. Prentice Hall, 1992.

[23] J. C. P. Woodcock and J. Davies. Using Z: specification, proof and refinement. Prentice Hall International Series in Computer Science, 1996.

[24] J. C. P. Woodcock, J. Davies, and C. Bolton. Abstract data types and processes. In J. Davies, A. W. Roscoe, and J. C. P. Woodcock, editors, Millennial perspectives in computer science: proceedings of the symposium in honour of Sir Tony Hoare. Palgrave, 2000.

[25] J. C. P. Woodcock and C. C. Morgan. Refinement of state-based concurrent systems. In D. Bjørner, C. A. R. Hoare, and H. Langmaack, editors, VDM and Z: Formal methods in software development. Springer, 1990.