Formal Aspects of Computing (1994) 6: 471–494
© 1994 BCS

Formal Aspects
of Computing

The Rest Stays Unchanged (Concurrency and State-Based Specification)

David Pitt[1] and Paddy Byers[2]

[1] Department of Mathematical and Computing Sciences, University of Surrey, UK and [2] Reference Information Systems, Ash Vale, Surrey, UK

Keywords: Boolean algebra; Concurrency; Pre-/postconditions

Abstract. Pre-/postconditions have been extensively used in program specification, e.g. Z [Spi89], VDM [Jon86], and proof, e.g. Hoare logic, Dijkstra's guarded commands [DiF88]. In [ScP86, SPB90] the authors introduced neutral and central relations to formalise the concept of "the rest stays the same". In this paper we abstract away from the specific definition of neutral relation given in [SPB90], through the mechanism of relational boolean algebras. This leads to the definition of implicitly central relations which are easier for the user in practical examples and facilitate the use of pre-/postcondition reasoning about truly concurrent behaviour.

1. Introduction

Model- or state-based styles of specification describe a system in terms of the state of the system and the effects of events on that state. The most popular Z [Spi89] and VDM [Jon86], follow this approach using pre- and postconditions to describe the relationship between the state before an event and that afterwards. This paper addresses a similar style first presented in [SPB90] but aims to extend previous work to include an interpretation of concurrent behaviour.

The intent in [SPB90] was that the specifier should be able to specify the effect of an event on just that part of the state in which he was interested and that, in the absence of other constraints, the rest of the state should remain unchanged. This permits the user to "underspecify" events, giving simpler more focused specifications.

Correspondence and offprint requests to: David Pitt, Department of Mathematical and Computing Sciences, University of Surrey, Guildford GU8 4UG, UK.

More importantly, context-sensitive interpretation of these "weak" postconditions gives a framework for building complex specifications by combining simpler components – each of which only constrains those parts of the state that it is genuinely interested in. Such compositionality is precluded by postconditions that are too "strong".

Neutral and central relations were defined to enable the specifier to make inferences about the whole state after an event, not just that part directly involved in the specification. Sections 2 and 3 of this paper introduce relational boolean algebras; these simple algebraic structures are then used in Section 4 to give the basic definitions of "the rest stays the same" for an event. The abstraction to relational boolean algebras facilitates the definition of implicitly central relations, which are in general very straightforward to construct for any specific event, and some very simple examples are given. Implicitly central relations embody that part of the state that the event is not concerned with, and thus give us the basis of a calculus for reasoning about overlapping occurrences of events. This view of concurrency is discussed in Section 6 using a simple result, on combining events, proved in Section 5. Sections 7 to 9 then consider the role of an invariant within the framework of relational boolean algebras.

2. Relational Boolean Algebras

Pre-/postcondition specifications are usually viewed as defining relations over sets of states, two states being related if the first satisfies the precondition and together they satisfy the postcondition. Thus if the state has a component S which is declared to be a set of natural numbers, the specification (true, $S' = S \cup \{1\}$) in which S' denotes the value of S after the event, would normally be satisfied by any pair of states provided $1 \in S$ in the second and that S was otherwise unchanged. Part of this relation is illustrated in Fig. 1. In the figure states are shown as models of set theory. A state in which $S = \{4, 5, 6\}$ is related under (true, $S' = S \cup \{1\}$) to a state in which $S = \{1, 4, 5, 6\}$. Whereas if we were to consider the relation specified by (true, $1 \in S'$) then the first state, whatever it was, would be related to any states in which 1 was an element of S.

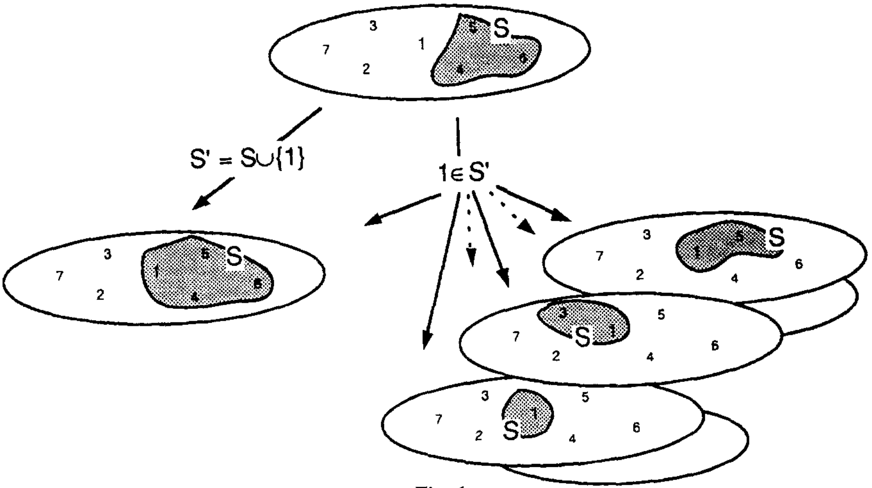
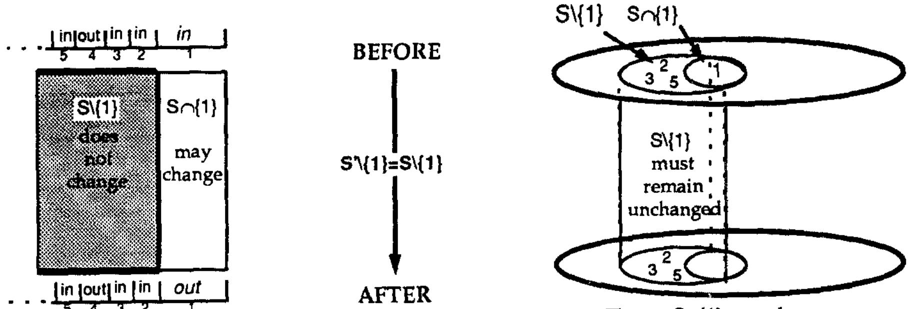


Fig. 1



The set S∩{1} may change.
In the picture it is {1} in the upper (pre)state
and the empty set, Ø, in the lower (post)state.

Fig. 2

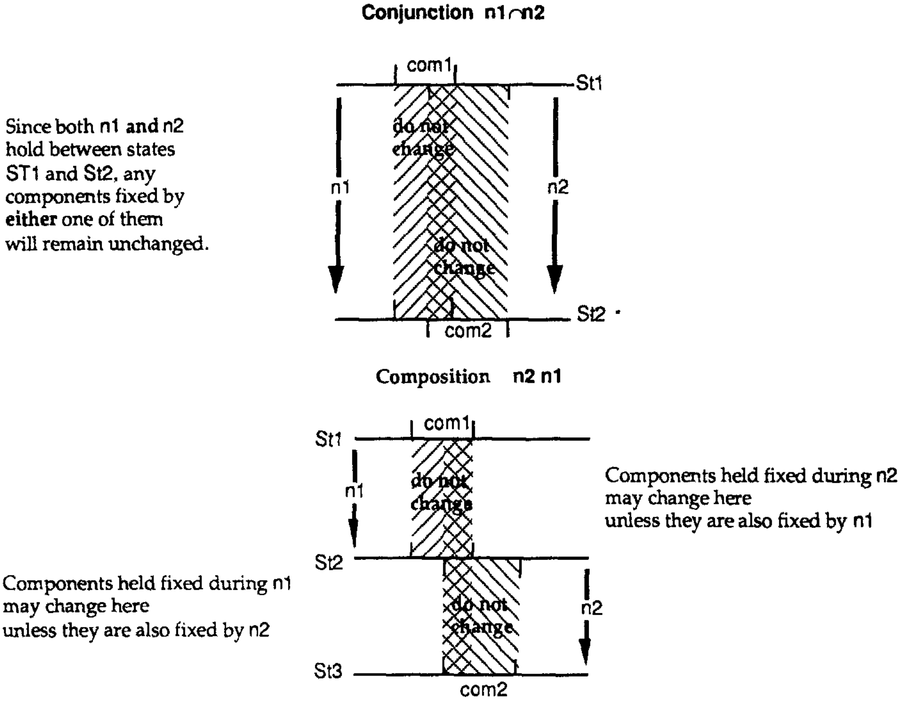
In [ScP86,90] neutral relations were introduced, these had no precondition and simply required that some component of state remained unchanged, for example (true, $X' = X$), two states would be related if the second could be obtained from the first leaving X unchanged, or (true, $S'\backslash\{1\} = S\backslash\{1\}$) in this case the presence or otherwise of elements other than 1 in S is required to remain unchanged. Figure 2 illustrates this in two ways that will be used throughout the paper. In both cases the horizontal layers represent possible states that may be related by the relation described on the vertical arrow. In the left-hand case components or parts of the state are schematically represented by sections of a horizontal line. On the right-hand side the state is intended to represent a world of sets; every component of the state will be represented by a set in that world. It is worth noting that we may use expressions in set theory to subdivide such components. Thus we may be interested in the set of elements of S which satisfy the predicate $x \neq 1$. The relation (true, $1 \in S'$), which would normally be satisfied by any pair of states provided $1 \in S$ in the second, could then be augmented by (true, $S'\backslash\{1\} = S\backslash\{1\}$) ensuring that the rest of S remains unchanged. A pair of states would satisfy the "augmented" specification just in case it satisfies both $1 \in S'$ and $S'\backslash\{1\} = S\backslash\{1\}$, that is $S' = S \cup \{1\}$.

If we view a neutral relation, n, as keeping fixed some component of state, *com*, then two states $st1$ and $st2$ will be related by n if $st2$ may be obtained from $st1$ by changing other components of state but leaving *com* fixed. Then $st1$ could be obtained from $st2$ in a similar manner and thus $st2$ and $st1$ would be related by n. This reversibility assumption about neutrals would lead to the conclusion that neutral relations should be *symmetric*.

If the neutral relations $n1$ and $n2$ kept fixed $com1$ and $com2$ respectively (see Fig. 3) and if $st1$ and $st2$ are related by $n1$ then $st2$ may be obtained from $st1$ leaving $com1$ fixed. Likewise if $st1$ and $st2$ are related by $n2$ then they agree on $com2$. Thus if $st1$ and $st2$ are related by both $n1$ and $n2$ then they must agree on both $com1$ and $com2$. That is $n1 \cap n2$ keeps both components, $com1 \cup com2$, fixed. Likewise, if any part of the state other tham $com1$ could change in the transition from $st1$ and $st2$ and anything other than $com2$ could differ from $st2$ to $st3$, then the only components of state where we could be sure $st1$ and $st3$ agree are those in the overlap of $com1$ and $com2$. Thus the relational composition[1] $n2\,n1$ keeps only the overlap, $com1 \cap com2$, fixed.

[1] We use $n2\,n1$ to denote the relation "do $n1$ then do $n2$" i.e. $(st1, st3) \in (n2\,n1)$, precisely when there is an $st2$ such that $(st1, st2) \in n1$ and $(st2, st3) \in n2$.

Components of state are represented schematically as sections of horizontal lines. Each horizontal line representing a state. The vertical axis may be viewed as the duration of the event. State components in unshaded areas may be changing.



Since both n1 and n2 hold between states ST1 and St2, any components fixed by **either** one of them will remain unchanged.

Components held fixed during n2 may change here unless they are also fixed by n1

Components held fixed during n1 may change here unless they are also fixed by n2

Fig. 3

From these observations we could conclude that if we had a complementation operation such that n^c kept fixed precisely those parts of the state which n permitted to change, then we would have a boolean algebra of symmetric relations, under relational composition, intersection of relations and the given complementation. (Note that this complementation will not be the complement of n within state × state i.e. (state × state)$\backslash n$.)

A *relational Boolean algebra* is a triple (W, N, C) where W is a (non-empty) set, N is a set of symmetric relations on W, and C is a function $C\colon N \to N$ (we write n^c for $C(n)$ the complement of n)), such that N forms a boolean algebra under C, intersection and composition with the relation $W \times W$ and the identity relation, I, as the respective identities. (Note that C is necessarily unique.)

The following properties of such an algebra will be used explicitly and are thus listed here. Properties R1, R2, R5, R6, R7, R8 and R9 are trivial and R3 follows from the symmetry of the relations involved. R4 may be seen as follows:

$$n = nI = n(m^c \cap m) = nm^c \cap nm \subseteq nm$$

Let (W, N, C) be a relational boolean algebra, then:

R1: N is closed under intersection and (relational) composition
R2: For all $n \in N$, $n^c \cap n = I$ the identity relation on W
R3: For all $n \in N$, $n^{-1}n^c = W \times W$ and $(n^c)^{-1}n = W \times W$
R4: For all $n, m \in N$, $n \subseteq nm$ and $n \subseteq mn$

R5: For all $n \in N$, $nn = n$
R6: For all $n, m \in N$, $(nm)^c = n^c \cap m^c$
R7: For any two elements $n, m \in N$, $nm = mn$
R8: For any three elements $n, m, r \in N$, $n(m \cap r) = nm \cap nr$
R9: For any three elements $n, m, r \in N$, $(m \cap r)n = mn \cap rn$

It follows from R2 and R5 above and the symmetry of the relations in N that the elements of a relational boolean algebra will always be equivalence relations.

Example 2.1. Let W be the set of all subsets of $\{1,2,3\}$, for each subset $A \subseteq \{1,2,3\}$ we define an equivalence relation n_A on W by $Xn_A Y \equiv_{\text{def}} X \cap A = Y \cap A$. Notice that $n_A n_B = n_{A \cap B}$ and $n_A \cap n_B = n_{A \cup B}$. Thus if we define $(n_A)^c \equiv_{\text{def}} n_{\{1,2,3\} \setminus A}$, and let N be the set of all the n_As, then (W, N, C) is a relational boolean algebra. Denote the above algebra by $\mathscr{RB}(\{1,2,3\})$.

If we considered the elements of W to be the values of a component of state, S, declared to be a subset of $\{1,2,3\}$, then n_A would correspond to the state to state relation keeping the intersection of S with A fixed;

i.e. $S' \cap A = S \cap A$ or $\{x \in S' \mid x \in A\} = \{x \in S \mid x \in A\}$.

Example 2.2. Given a relational model for pre-/postcondition set theoretic specifications, then let W be the set of "states" and let N be the set of relations corresponding to conjunctions of postconditions of the form $P_{\Phi,X} \equiv_{\text{def}} \{x \in X' \mid \Phi(x)\} = \{x \in X \mid \Phi(x)\}$, where X is a state variable and $\Phi(x)$ is a formula from the underlying language of set theory together with the so-called given set names but not involving the state variable names. Then, if we define $(P_{\Phi,X}) \equiv_{\text{def}} P_{-\Phi,X}$, (W, N, C) is a relational boolean algebra. (Note that the composition of the relations corresponding to $P_{\Phi,X}$ and $P_{\Theta,X}$ is the relation corresponding to $P_{\Phi \wedge \Theta,X}$ and that corresponding to their intersection is $P_{\Phi \vee \Theta,X}$.) Figure 4 shows $P_{\Phi,X} \cap P_{\Theta,Y}$. It keeps fixed the set of elements in X that satisfy Φ and those of Y that satisfy Θ; the presence or otherwise of elements in X and Y not satisfying these predicates may change.

It is worth observing that the fact that n^c is the complement of n within the boolean algebra (i.e. $nn^c = W \times W$) means that for any pair of elements of W (states), w_0, w_1, there is another $w \in W$ such that $w_0 nw$ and $wn^c w_1$. However since n and n^c are both symmetric and idempotent, we have $nn^{-1} = n$ and $(n^c)^{-1} n^c = n^c$ and so consideration of the following figure shows that if w' were another possible

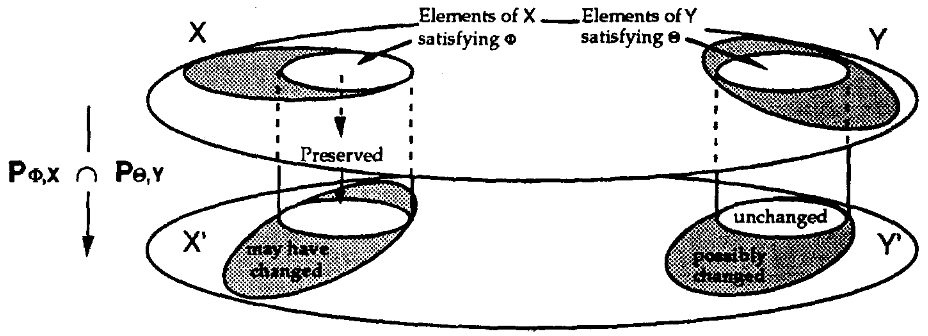


Fig. 4

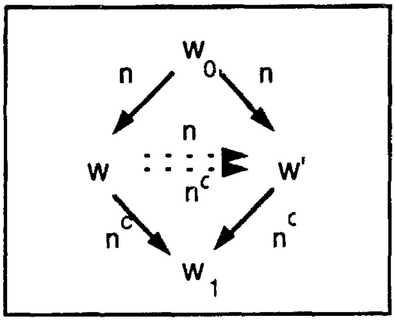


Fig. 5

intermediate state then $w(n^c \cap n)w'$. But $n^c \cap n = I$ thus the intermediate state is unique (Figure 5). It is the state which agrees with w_0 "on that part of the state" fixed by n and with w_1 on the rest.

3. Representation Results for Relational Boolean Algebras

Our principle concern is with relational boolean algebras of the form described in Examples 2.1 and 2.2 above. In this section we investigate briefly how typical these examples are.

Proposition 3.1. Every boolean algebra is isomorphic to the underlying boolean algebra of a relational boolean algebra.

Proof. Let $(B, \wedge, \vee, ', 1, 0)$ be a boolean algebra, and let S be a set and A a set of subsets of S such that $(A, \cap, \cup, ^c, S, \emptyset)$ forms a boolean algebra isomorphic to $(B, \wedge, \vee, ', 1, 0)$ the existence of S and A is guaranteed by Stone's theorem, see for example [DaP90]. Form a relational boolean algebra as follows (W, N, C), let $W = A$ and let $N = \{r_b \subseteq W \times W\colon b \in A\}$ where $r_b = \{(b1, b2) \in W \times W\colon b1 \cap b = b2 \cap b\}$ then the underlying boolean algebra of (W, N, C) is isomorphic to $(A, \cap, \cup, ^c, S)$, under the function, $r_b \mapsto b$, and thus to $(B, \wedge, \vee, ', 1, 0)$. □

A *weak $\mathcal{RB}$-representation* of a relational boolean algebra, (W, N, C), is a set A together with two one-one functions,

$$rep_w\colon W \to \mathcal{P}(A) \text{ and } rep_N\colon N \to \mathcal{P}(A)$$

such that

$$(w_1 n w_2) \Leftrightarrow (rep_w(w_1) \cap rep_N(n) = rep_w(w_2) \cap rep_N(n))$$

Proposition 3.2. Every relational boolean algebra, (W, N, C), has a weak $\mathcal{RB}$-representation.

Proof. For each element $n \in N$ let A_n denote the set of equivalence classes of n. Let A be the disjoint union $(\bigsqcup_{n \in N} A_N) \bigsqcup W$. We define $rep_N(n) = A_n$ and $rep_w(w) = \{[w]_n \in A \mid n \in N\} \cup \{w\}$ where $[w]_n$ is the equivalence class of w under n. Then $rep_w(w) \cap rep_N(n) = \{[w]_n\}$. The required result follows. □

It should be noted that the representation function defined in the above proof will not determine a boolean algebra homomorphism from the underlying boolean algebra of (W, N, C) to that of $\mathcal{RB}(A)$.

A *strong $\mathscr{RB}$-representation* of a relational boolean algebra, (W, N, C) is a weak $\mathscr{RB}$-representation in which $rep_N\colon N \to \mathscr{P}(A)$ yields a boolean algebra homomorphism.

We are not able to prove that all relational boolean algebras have a strong $\mathscr{RB}$-representation. However, we do have the following theorem; a similar result has been proved for an equivalent model in [Shi91a].

Proposition 3.3. Every relational boolean algebra, (W, N, C), in which N is closed under arbitrary intersections, has a strong $\mathscr{RB}$-representation.

Proof. Let A be a set and $rep\colon N \to \mathscr{P}(A)$ be a boolean algebra monomorphism such that

$$rep(n_1 n_2) = rep(n_1) \cap rep(n_2) \text{ and } rep(n_1 \cap n_2) = rep(n_1) \cup rep(n_2)$$

Let $rep_N\colon N \to \mathscr{P}(A \times W)$ be defined by $rep_N(n) = rep(n) \times W$; note rep_N is also a boolean algebra monomorphism, and let $rep_W\colon W \to \mathscr{P}(A \times W)$ be defined by

$$rep_W(w) = \{(a, w') \in A \times W \mid \exists n \in N . a \in rep(n) \wedge (wnw')\}$$

Then

$$rep_W(w) \cap rep_N(n) = rep_N(n) \times [w]_n$$

and so for $n \neq W \times W$ we have $rep_N(n) \neq \varnothing$ and thus;

$$\begin{aligned} & rep_W(w) \cap rep_N(n) = rep_W(w') \cap rep_N(n) \\ & \Leftrightarrow rep_N(n) \times [w]_n = rep_N(n) \times [w']_n && \text{(note } rep_N \text{ is one-one)} \\ & \Leftrightarrow [w]_n = [w']_n \\ & \Leftrightarrow wnw' \end{aligned}$$

and $rep_N(W \times W) = \varnothing$, whence

$$rep_W(w) \cap rep_N(n) = rep_W(w') \cap rep_N(n) \Leftrightarrow wnw'$$

Thus if rep_W is one-one we have a strong representation.

Notice $rep(I) = A$ and so $A \times \{w\} \subseteq rep_W(w)$, thus if $rep_W(w) = rep_W(w')$, then we have

$$A \times \{w'\} \subseteq rep_W(w)$$

so for each $a \in A$ we have $n_a \in N$ such that $a \in rep(n_a)$ and $wn_a w'$.

By monotonicity of rep we have

$$rep(n_a) \subseteq rep(\bigcap_{a \in A} n_a)$$

and thus

$$A = \bigcup_{a \in A} rep(n_a) \subseteq rep(\bigcap_{a \in A} n_a)$$

whence

$$rep(\bigcap_{a \in A} n_a) = A = rep(I)$$

and since rep is one-one,

$$I = \bigcap_{a \in A} n_a$$

but $wn_a w'$ for each n_a, thus $w = w'$. So rep_W is one-one. □

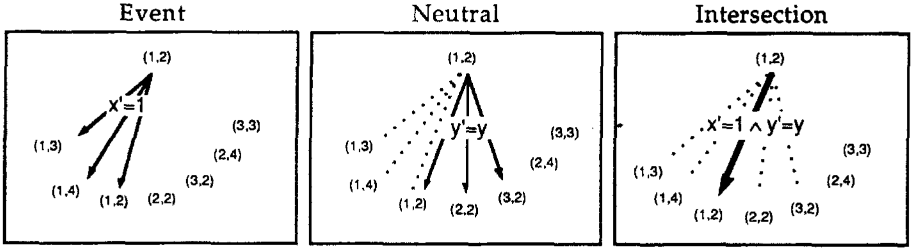


Fig. 6

4. Relational/Neutral Systems and Central Relations

A *relational/neutral* system is a quadruple (W, E, N, C) where (W, N, C) is a relational boolean algebra and E is a set of relations on W. The elements of E are called *events* and those of N are termed *neutral events* or simply *neutrals*.

The intent is to use neutral relations to augment underspecified events to define a sound concept of "the rest stays unchanged". Suppose for example we have two state components, (x, y), and we wish to define the event x becomes equal to 1. If we write $x' = 1$, then for any pre-state the relation defined yields too many poststates, as illustrated in Fig. 6. We wish to restrict those states by demanding that as much as possible of the state should remain unchanged, while sustaining at least one possible poststate.

A neutral event n is said to be *consistent* with an event e precisely if the domain of $e \cap n$ is equal to the domain of e.

We also require that all such "rest stays unchanged" assumptions are mutually consistent. That is, if we take two of them together with the event in question we do not lose the possibility of a poststate.

A neutral event m is said to be *central* to an event e precisely if m is consistent with $e \cap n$ for any neutral n which is consistent with e. Thus if we view $e \cap m$ as an implementation then for every possible prestate and any other implementation there will be at least one poststate shared by both implementations.

The set of neutral relations that are consistent with, central to an event e will be denoted by *consistent*(e) and *central*(e) respectively. Notice that *central*(e) is closed under intersections whereas consistent(e) may not be. Both are closed under composition.

Example 4.1 (2.1 *revisited*). Let W be the set of all subsets of $\{1, 2, 3\}$, with N and C as before and let E be the set of all relations on W. The relations in E may be thought of as non-deterministic events and any subset $X \subseteq \{1, 2, 3\}$ may be considered as the value of a set-valued variable. The sets Y such that XeY may then be viewed as possible values of the variable after an occurrence of the event e from an initial value X. Then the neutral event n_A may be thought of as an event which simply insists that the presence or otherwise of the various elements of A in the variable is the same after an occurrence as it was before, but that elements not in A may be added or removed.

Consider the relation given by $Xe1\,Y \equiv_{\text{def}} 1 \in Y$. This insists that 1 is in the set afterwards but does not care about any other elements. Then

$$consistent(e1) = \{n_\varnothing, n_{\{2\}}, n_{\{3\}}, n_{\{2,3\}}\}$$

since we can always sustain the presence or otherwise of various elements of the set other than 1 and still insist that 1 is in afterwards. These consistent relations are all mutually consistent with $e1$ thus

$$\mathit{central}(e1) = \mathit{consistent}(e1)$$

If we consider the relation given by $Xe2Y \equiv_{\mathrm{def}} 1 \in Y \vee 2 \in Y$. Then

$$\mathit{consistent}(e2) = \{n_{\varnothing}, n_{\{1\}}, n_{\{2\}}, n_{\{3\}}, n_{\{1,3\}}, n_{\{2,3\}}\}$$

so, for example, you can always force 1 or 2 to be in afterwards, keeping the presence or otherwise of 1 the same and likewise with the presence of 2, but not both together. Thus

$$\mathit{central}(e2) = \{n_{\varnothing}, n_{\{3\}}\}$$

Example 4.2 (2.2 *revisited*). If we allow our set of events, E, to range over all (precondition, postcondition) pairs in a suitable language, then a neutral is consistent with the event precisely if whenever from some initial state a suitable poststate exists for the event then it is possible to move from the initial state to a poststate without changing the components of state that the neutral keeps fixed.

Central relations are intended to keep fixed those parts of the state that the specifier was not primarily concerned with. These could be defined as those whose contamination during the event would not violate the postcondition of the event. We could define that part of the state which was "of interest" as that which if held unchanged on conclusion of the event would preserve the postcondition, as illustrated in Fig. 7.

One could argue that the rest, "the complement of that which the specifier is interested in", should remain untouched by the event. This combination of preservation and complementation will yield a simple means of extracting central relations for events. A relation r *preserves* a relation e if $re \subseteq e$ (Fig. 8). Since

$$(r \cap p)e \subseteq re \cap pe$$

and

$$(re \subseteq e \wedge pe \subseteq e) \Rightarrow (rpe \subseteq re \subseteq e)$$

we have the following.

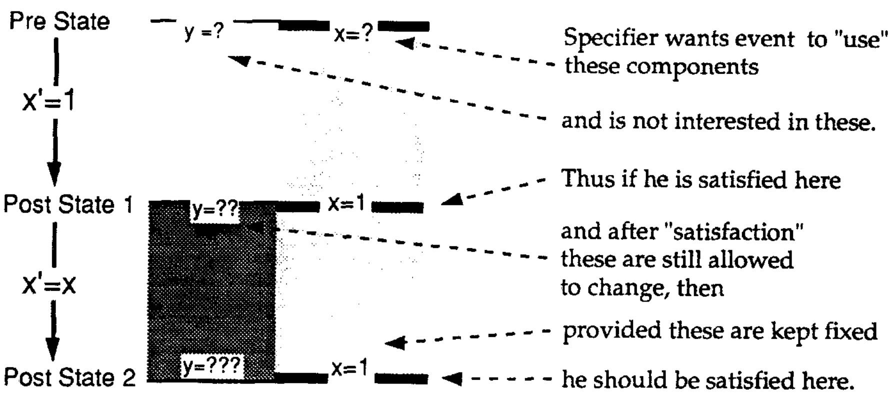
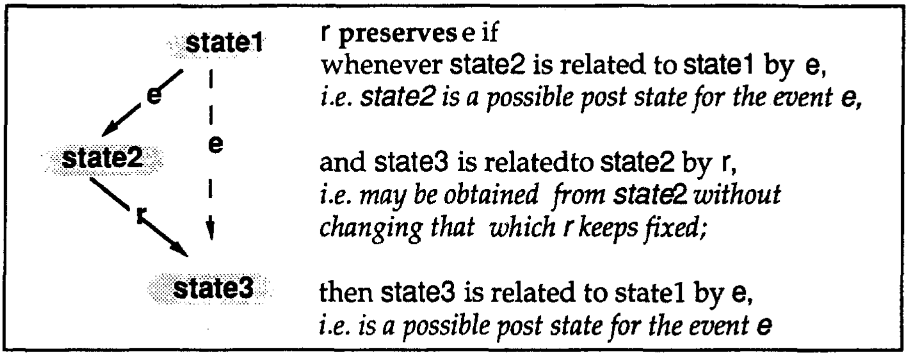

Pre State
X'=1
Post State 1
X'=X
Post State 2
y =?
x=?
y=??
x=1
y=???
x=1
Specifier wants event to "use" these components
and is not interested in these.
Thus if he is satisfied here
and after "satisfaction" these are still allowed to change, then
provided these are kept fixed
he should be satisfied here.

Fig. 7



r preserves e if
whenever state2 is related to state1 by e,
i.e. state2 is a possible post state for the event e,

and state3 is relatedto state2 by r,
i.e. may be obtained from state2 without changing that which r keeps fixed;

then state3 is related to statel by e,
i.e. is a possible post state for the event e

Fig. 8

Proposition 4.1. If r and p preserve e then so do $r \cap p$ and rp.

If n is a neutral relation such that n^c preserves e then n is termed *implicitly-central* to e (Fig. 9). In Example 4.1 above, $n_{\{1\}}$ and $n_{\{1,2\}}$ preserve $e1$ and $e2$ respectively. Thus $(n_{\{1\}})^c = n_{\{2,3\}}$ and $(n_{\{1,2\}})^c = n_{\{3\}}$ are implicitly central to $e1$ and $e2$ respectively.
As a consequence of Proposition 4.1 we have the following.

Proposition 4.2. If n and m are implicitly central to e then so are $n \cap m$ and nm.

We are now in a position to prove the main result of this section justifying the introduction of the above definition.

Proposition 4.3. If n is implicitly-central to e then n is central to e.

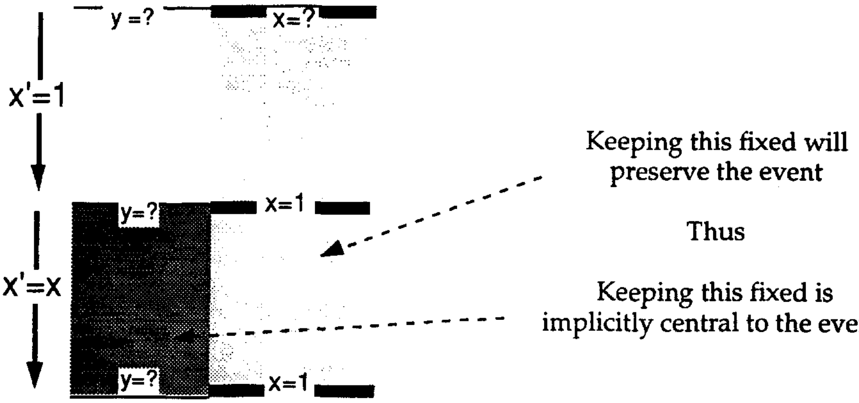
Proof. Let n be implicitly equal to e and let m be consistent with e. Let

$$\alpha \in dom(e \cap m) = dom(e) \quad \text{(since } m \text{ is consistent with } e\text{)}$$

then we have β such that $\alpha e \beta$ and $\alpha m \beta$. But

$$(n^c)^{-1} n = W \times W \quad \text{(R3)}$$

thus we have δ such that $\beta n^c \delta$ and $\alpha n \delta$ (Fig. 10).



Keeping this fixed will preserve the event

Thus

Keeping this fixed is implicitly central to the event.

Fig. 9

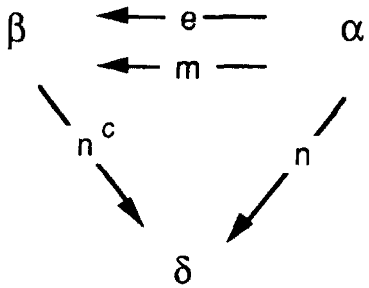


Fig. 10

So, since n^c preserves e, $\alpha e \delta$ by R4:

$$\beta(n^c)\,\delta \text{ yields } \beta(n^c m)\,\delta \text{ and } \alpha(m)\,\beta \text{ yields } \alpha(n^c m)\,\beta$$

and thus by R5:

$$\alpha(n^c m)\,\delta$$

and by R4: since $\alpha n \delta$ we have $\alpha(nm)\,\delta$. Thus

$$\alpha(n^c m \sqcap nm)\,\delta$$

But we have

$$\begin{aligned} m &= Im \\ &= (n^c \sqcap n)\,m && \text{(R2)} \\ &= n^c m \sqcap nm \end{aligned}$$

and so $\alpha m \delta$. Thus

$$\alpha \in dom(e \sqcap m \sqcap n)$$

and so $m \sqcap n$ is consistent with e. □

In general it is more straightforward to show that a neutral is implicitly central to a relation than to show that it is actually central. This is illustrated by the following example.

Example 4.2 (*continued*).
The relation $\{x \in X' \mid x = 1 \vee x = 2\} = \{x \in X \mid x = 1 \vee x = 2\}$ preserves $e = (\text{true}, \{1,2\} \subseteq X')$. Thus $\{x \in X' \mid x \neq 1 \wedge x \neq 2\} = \{x \in X \mid x \neq 1 \wedge x \neq 2\}$, or $X' \backslash \{1,2\} = X \backslash \{1,2\}$, is implicitly central to e and thus central to e.

5. Relations Implicitly Central to Combined Events

Section 6 will consider the possibility of two or more events occurring concurrently. In that context it will be necessary to consider neutrals which are central to the resulting combinations of events. This is considered in Proposition 5.2 below.

Lemma 5.1. If n and m preserve e and f respectively then $n \sqcap m$ preserves $e \sqcap f$.

Proof. Assume $\alpha(e \sqcap f)\,\beta$ and $\beta(n \sqcap m)\,\delta$. Then we have $\alpha e \beta$ and $\beta n \delta$ and since n preserves e we have $\alpha e \delta$, and we have $\alpha f \beta$ and $\beta m \delta$ and since m preserves f we have $\alpha f \delta$. Whence $\alpha(e \sqcap f)\,\delta$ (see Fig. 11). So $n \sqcap m$ preserves $e \sqcap f$. □

Recall that N satisfies, R6, i.e. for all $n, m \in N$, $(nm)^c = n^c \sqcap m^c$. Thus we have the following.

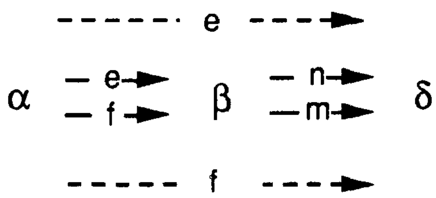


Fig. 11

Proposition 5.2. If n_1 and n_2 are implicitly central to e_1 and e_2 respectively, then $n_1 n_2$ is implicitly central to $e_1 \cap e_2$.

Proof. Let n_1 and n_2 be implicitly central to e_1 and e_2 respectively. Then n_1^c preserves e_1 and n_2^c preserves e_2. Thus by the lemma $n_1^c \cap n_2^c$ preserves $e_1 \cap e_2$. But

$$(n_1 n_2)^c = n_1^c \cap n_2^c \tag{R6}$$

and thus $n_1 n_2$ is implicitly central to $e_1 \cap e_2$. □

6. Reasoning About Concurrent Behaviour

Thus far we have considered relations as events linking states before an occurrence to those reachable afterwards. This view has tended to treat events as atomic, in that there is no notion of possible states between the start of an event and its completion. In such a view of the world the only form of concurrency that we can address is synchronisation/handshaking, where events occur at the same time, and/or interleaving events in arbitrary orderings. This was the view taken in [SPB90] and is also consistent with the approach in most process algebras, such as CSP, CCS, LOTOS [Hoa85, Mil89, EVO89]. Here the approach is closer to that in [Shi91b] which gives "true concurrency" operational semantics to a related model.

The concept of implicitly central relations enables us to consider possible intermediate states, between the start and finish of an event. This will then enable us to consider the possibility of reasoning about overlapping events as illustrated in Fig. 12.

We adopt the view that the event is only concerned with those components of state which are kept fixed by all relations that preserve that event and so it will not interfere with any that are kept fixed by the complement of any such relation. Consider the example given in Fig. 6.

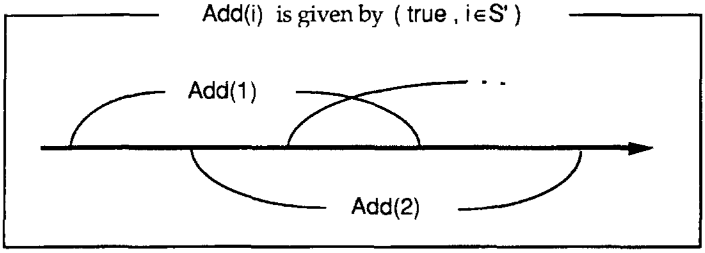
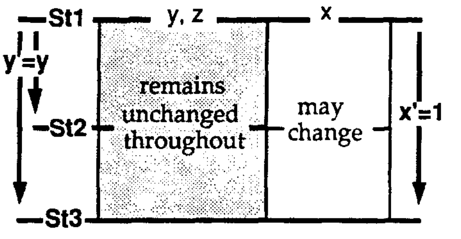


Fig. 12



If we keep x fixed after completion of the event x'=1 then x will continue to equal 1. Thus the event is preserved by the relation x'=x, and we assume that it is only concerned with the variable, x. Thus we assume that the variable y is unchanged at any intermediate state, but x may have changed.

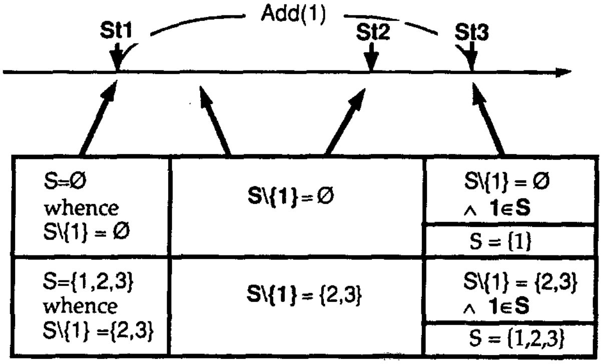
Fig. 13

We may conclude that if *St*1 is a start state for an event then *St*2 is a possible intermediate state just in case *St*1 and *St*2 are related by every relation which is implicitly central to that event, as shown in Fig. 13. Notice that since all neutrals contain the identity relation *St*1 itself is always a candidate. This may be viewed as being similar to the guarantee conditions of Jones [Jon83, WoD88], in that the first event guarantees not to disturb those components of state fixed by implicitly central relations.

Returning to the context of Example 4.2, we consider the event, *Add*(1), inserting 1 into the set S; then 1 will continue to be an element of S provided we keep $S \cap \{1\}$ fixed. We have, $S' \cap \{1\} = S \cap \{1\}$ preserves *Add*(1) and thus $S' \backslash \{1\} = S \backslash \{1\}$ is implicitly central. So at any intermediate state, *St*2, we may infer any property of *St*1 preserved by $S' \backslash \{1\} = S \backslash \{1\}$. On completion of the event, at *St*3, we may infer all such properties and anything implied by the postcondition. The consistency of such conclusions is guaranteed by Proposition 4.3. Some examples are shown in Fig. 14.

If on the other hand we were to consider an event *put*(1) with postcondition $put(1) \equiv S' \cap \{1, 2, 3\} = (S \cap \{1, 2, 3\}) \cup \{1\}$. Then $n_{\{2,3\}} \equiv S' \cap \{2, 3\} = (S \cap \{2, 3\})$ is central to the event, in fact $put(1) \Rightarrow n_{\{2,3\}}$, or thinking of the associated relations between states we have $put(1) \subseteq n_{\{2,3\}}$. The event explicitly requires $S \cap \{2, 3\}$ to remain unchanged.

In the case of a general relational neutral system a neutral, n, is said to be *explicitly central* to an event, e, just in case $e \subseteq n$. Thus if view then the component of state corresponding to n in v is unchanged by e. The following proposition



S=∅ whence S\{1} = ∅	S\{1}=∅	S\{1} = ∅ ∧ 1∈S S = {1}

S={1,2,3}
whence
S\{1} ={2,3}
	S\{1} = {2,3}	S\{1} = {2,3}
		∧ 1∈S
		S = {1,2,3}

Fig. 14

guarantees that implicitly and explicitly central relations are concerned with disjoint components of state.

Proposition 6.1. When n_1 and n_2 are relations which are respectively implicitly and explicitly central to a non-empty event e then $n_1 n_2 = W \times W$.

Proof. Let $r = n_1^c$. Then r preserves e and so $re \subseteq e \subseteq n_2$. Thus $n_1 re \subseteq n_1 n_2$. But

$$n_1 r = n_1 n_1^c = W \times W \text{ and } (W \times W)e = dom(e) \times W$$

and so $dom(e) \times W \subseteq n_1 n_2$. But $n_1 n_2$ is symmetric and transitive, so since $dom(e) \neq \emptyset$ we have $W \times W \subseteq n_1 n_2$.

We take the view that we should not assume that $put(1)$ does not interfere with $S \cap \{2, 3\}$, in fact if someone else does during the course of an occurrence of $put(1)$ then it will have to re-establish the initial value of $S \cap \{2, 3\}$ on termination in order to satisfy its postcondition. Thus we may consider components of state fixed by explicitly central relations as having been "copied and rewritten" and those fixed by implicitly central relations as having been "untouched".

We may now consider overlapping events; we will not propose a specific model for concurrency, rather we suggest how implicitly central relations may be used to reason about the state when events occur independently. In a relational neutral system, (W, E, N, C), let $e1$ and $e2$ be events and let $n1$ and $n2$ be any two neutrals implicitly central to $e1$ and $e2$ respectively. If we assume that the state, i.e. a member of W, is changing over time and that $e1$ and $e2$ start and finish as indicated in Fig. 15. What can we infer about the various states indicated?

$St1$ is in the domain of $e1$.

> "$e1$ can start."

$St2$ is related to $St1$ by $n1$.

> "The components of state fixed by $n1$ remains unchanged..."

$St3$ is in the domain of $e2$ and is related to $St1$ by $n1$.

> "...and $e2$ can start...."

$St4$ is related to $St3$ by $n2n1 = n1n2$.

> "...Only those components of state that both $e1$ and $e2$ guarantee to leave unchanged may be assumed to stay the same, (Recall that $n2n1$ keeps fixed the intersection of those components fixed by $n1$ and $n2$)..."

$St5$ is related to $St3$ by $(n2n1)$ and $St5$ is related to $St1$ by $e1$.

> "...and the postcondition of $e1$ holds."

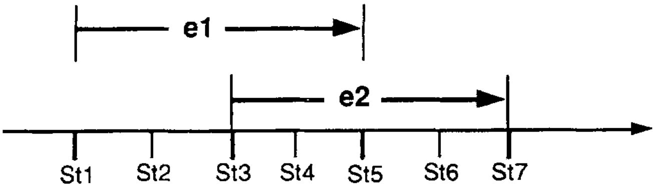


Fig. 15

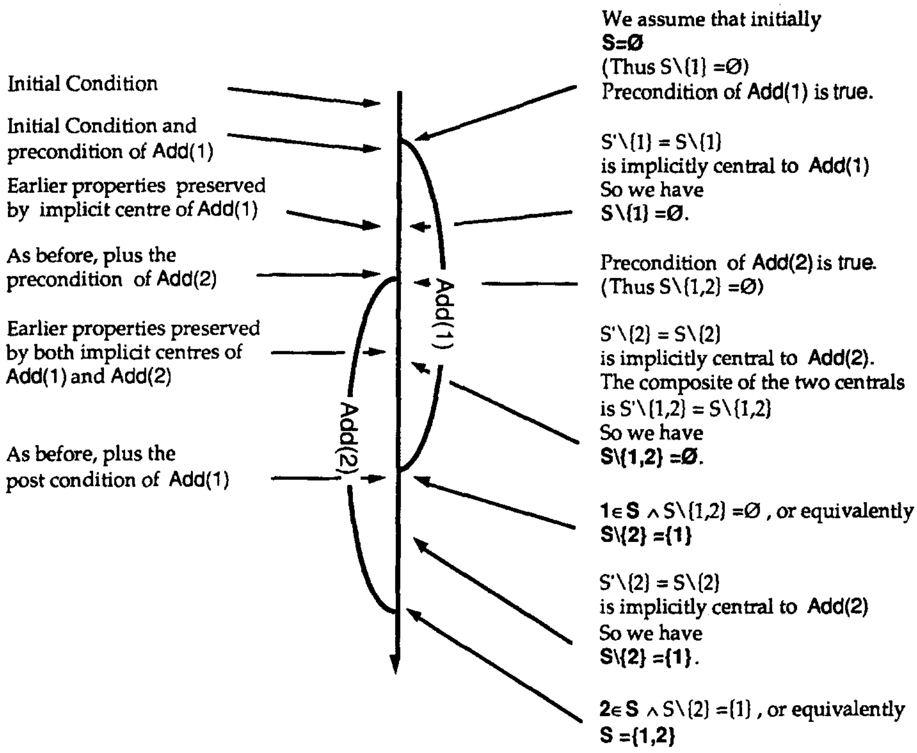

Initial Condition
Initial Condition and precondition of Add(1)
Earlier properties preserved by implicit centre of Add(1)
As before, plus the precondition of Add(2)
Earlier properties preserved by both implicit centres of Add(1) and Add(2)
As before, plus the post condition of Add(1)
Add(1)
Add(2)
We assume that initially
S=∅
(Thus S\{1} =∅)
Precondition of Add(1) is true.
S'\{1} = S\{1}
is implicitly central to Add(1)
So we have
S\{1} =∅.
Precondition of Add(2) is true.
(Thus S\{1,2} =∅)
S'\{2} = S\{2}
is implicitly central to Add(2).
The composite of the two centrals
is S'\{1,2} = S\{1,2}
So we have
S\{1,2} =∅.
1∈S ∧ S\{1,2} =∅ , or equivalently
S\{2} ={1}
S'\{2} = S\{2}
is implicitly central to Add(2)
So we have
S\{2} ={1}.
2∈S ∧ S\{2} ={1} , or equivalently
S ={1,2}

Fig. 16

$St6$ is related to $St5$ by $n2$.
$St7$ is related to $St5$ by $n2$ and $St7$ is related to $St3$ by $e2$.

Example 6.2 (*4.2 continued*). We now consider the example where $e1$, $e2$, $n1$ and $n2$ are $add(1) \equiv (\text{true}, 1 \in S')$, $add(2) \equiv (\text{true}, 2 \in S')$, $(\text{true}, S'\backslash\{1\} = S\backslash\{1\})$, and $(\text{true}, S'\backslash\{2\} = S\backslash\{2\})$ respectively, and the composite relation $n1n2$ is $(\text{true}, S'\backslash\{1,2\} = S\backslash\{1,2\})$ (Figure 16). Within this framework we can then reason about the state after events occur concurrently. We give just two examples.

In (W, E, N, C) two events, $e1$ and $e2$, may be termed *independent* if whenever they overlap or occur concurrently, in the absence of any other interference, then the state reached after they have both finished is related to the states at which they respectively started by the relations $e1$ and $e2$. Thus in Fig. 17 we require that $St3$ is related to $St1$ by $e1$ and $St3$ is related to $St2$ by $e2$ in all cases.

If we assume the inference rules, for intermediate states, stated above we have the following.

Proposition 6.2. When n_1 and n_2 are relations which are implicitly central to $e1$ and $e2$ respectively, and preserve $e2$ and $e1$ respectively, then $e1$ and $e2$ are independent.

Proof. In every case $St3$ is related to $St1$ by either $e1$ or $n2e1$ but since $n2$ preserves $e1$ they are related by $e1$ in both cases. A similar argument shows that $ST3$ is related to $St2$ by $e2$ in all cases. □

In Example 6.2, $S'\backslash\{2\} = S\backslash\{2\}$ preserves $1 \in S'$ and $S'\backslash\{1\} = S\backslash\{1\}$ preserves $2 \in S'$. Thus $Add(1)$ and $Add(2)$ are independent.

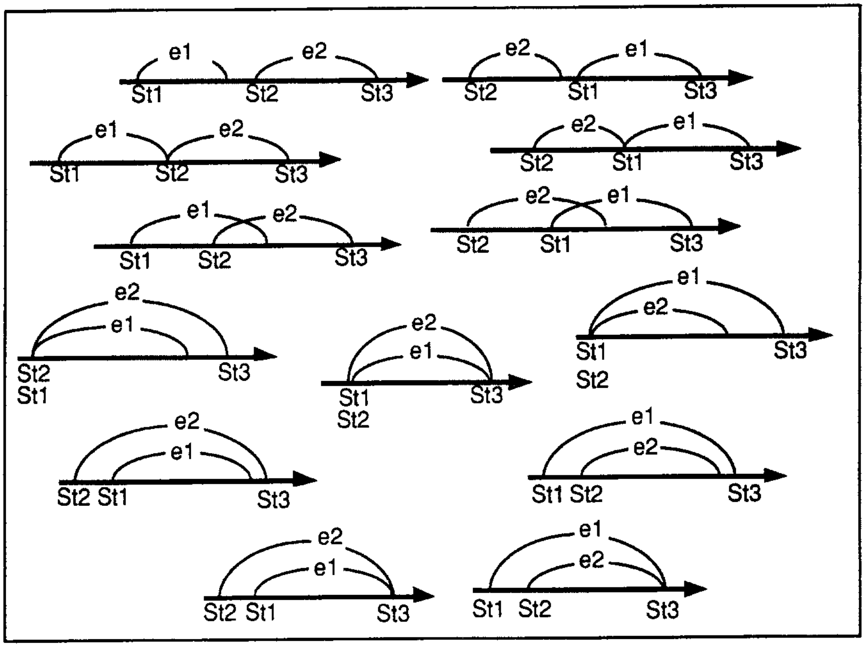


Fig. 17

For our second example we consider a stronger form of independence. In (W, E, N, C) two events, $e1$ and $e2$, may be termed *strongly independent* if whenever they overlap or occur concurrently, in the absence of any other interference, then the state reached after they have both finished is related to the state at which they first started by the relations $e1$ and $e2$.

If we say that a neutral n *strongly preserves* relation e if n preserves e and $en \subseteq e$, then we have the following.

Proposition 6.3. When n_1 and n_2 are relations which are implicitly central to $e1$ and $e2$ respectively, and strongly preserve $e2$ and $e1$ respectively, then $e1$ and $e2$ are strongly independent.

Proof. In every case $St3$ is related to $St0$, where $St0$ is the leftmost state in the diagram, by either $e1$, $n2e1$, $e1n2$ or $n2e1n2$ but since $n2$ strongly preserves $e1$ they are related by $e1$ in all cases. A similar argument shows that $St3$ is related to $St2$ by $e2$ in all cases. □

In Example 6.2, $S'\backslash\{1\} = S\backslash\{1\}$ strongly preserves $1 \in S'$ and $S'\backslash\{2\} = S\backslash\{2\}$ strongly preserves $2 \in S'$. Thus *Add*(1) and *Add*(2) are strongly independent.

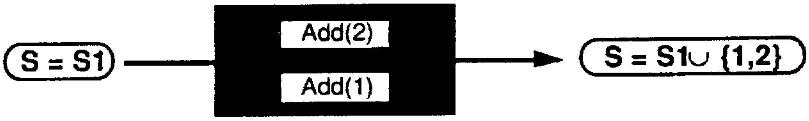


Fig. 18

Since the composite of the two centrals is $S'\backslash\{1,2\} = S\backslash\{1,2\}$ we have, in the absence of any other interference, if the two events occur in any order then the state before the occurrences and that after are related by $1 \in S' \wedge 2 \in S' \wedge S'\backslash\{1,2\} = S\backslash\{1,2\}$ i.e. $S' = S \cup \{1,2\}$ as shown in Fig. 18.

7. Systems with Invariant

In the style of specification discussed in [SPB90], the state is subject to an invariant and the definition of an event is automatically augmented to re-establish the invariant. For example we may have a component of state, $f: A \to A$ which is declared to be a function from A to A. Then an event $f'(a) = b$ may be defined with the intention of establishing the value of $f(a)$ to be b while still requiring that f' is a function. Thus the explicit postcondition is intended to be $(f'(a) = b) \wedge (f' \in A \to A)$. To preserve this postcondition it would be necessary to keep the whole of f fixed, since f is only a set of pairs and we would need to preserve its functionality. Thus we get no useful implicitly central relation, even though it is in fact possible to prove that

$$\{(x,y) \in f' \mid x \neq a\} = \{(x,y) \in f \mid x \neq a\}$$

i.e. $\forall x \neq a . f'(x) = f(x)$, is central to $(f'(a) = b) \wedge (f' \in A \to A)$. The specifier of the event was really only interested in the value of $f(a)$ after the event, expecting the invariant to be sustained. We wish to use the fact that

$$R \equiv_{\text{def}} \{(x,y) \in f' \mid x = a\} = \{(x,y) \in f \mid x = a\} \text{ preserves } f'(a) = b$$

to conclude that

$$R^c \equiv \{(x,y) \in f' \mid x \neq a\} = \{(x,y) \in f \mid x \neq a\} \text{ is central to } (f \in A \to A) \wedge (f'(a) = b) \wedge (f' \in A \to A)$$

It transpires that this will work because R respects the invariant in the sense that if we restrict attention to states which satisfy the invariant, i.e. in which f is a function, then R becomes $f'(a) = f(a)$ and R^c becomes $\forall x \neq a . f'(x) = f(x)$. These keep disjoint components of state fixed. The first places no restriction on the way $f(x)$ may be changed when $x \neq a$, and these values of $f(x)$ are precisely those which are kept fixed by the second. The second places no restriction on the way $f(a)$ may be changed and this value is precisely that which is kept fixed by the first. So R and R^c remain complementary when restricted to states in which f is a function.

Essentially, it is possible to split the invariant over the state into a part over the components of state fixed by R, requiring that f restricted to $\{a\}$ is a function, and a part over the components of state fixed by R^c, requiring that f restricted to $A\backslash\{a\}$ is a function, such that if both parts are satisfied then the whole invariant is also satisfied.

The relation $P \equiv_{\text{def}} \{(x,y) \in f' \mid x = y\} = \{(x,y) \in f \mid x = y\}$ (Fig. 19) does not respect the invariant in this way. P would preserve the event $f'(a) = a$. However its complement is not even consistent with $(f \in A \to A) \wedge f'(a) = a \wedge (f' \in A \to A)$, since it is possible that in the previous state $f(a) \neq a$.

A *relational/neutral system with invariant* is a quintuple (W, E, N, C, inv) where the first four components are as before and *inv* is simply a subset of W (or a unary relation on W). Consistent/Central neutrals may now be defined as before but with respect to $e \cap (inv \times inv)$, the latter being the intended basic event since events are to be required to preserve the invariant.

		Restricted to states in which f is a function	
P	$\{(x,y)\in f' \mid x=y\} = \{(x,y)\in f \mid x=y\}$	$f(x)=x \vee f'(x)=x \Rightarrow f'(x) = f(x)$	The restriction permits f(x) to change provided f(x)≠x and the change is restricted so that f'(x)≠x.
P^c	$\{(x,y)\in f' \mid x\neq y\} = \{(x,y)\in f \mid x\neq y\}$	$f(x)\neq x \vee f'(x)\neq x \Rightarrow f'(x) = f(x)$	If f(x) = x then, apparently, f(x) may change but not into a state where f(x)≠ x. Thus in fact this restriction keeps the whole of f fixed.

Fig. 19

For any relation $r \subseteq W\times W$ we define $r^i =_{\text{def}} r \cap (inv \times inv) \subseteq inv \times inv$. Note $r^i \cap q^i = (r \cap q)^i$, but in general $r^i q^i \neq (rq)^i$.

In the above examples the invariant is $f\in A \to A$, so we are restricting to states in which f is a function, then[2]

$$R^i \equiv f'(a) = f(a), \quad (R^c)^i \equiv \forall x \neq a . f'(x) = f(x)$$
$$P^i \equiv \forall x . ((f(x) = x \vee f'(x) = x) \Rightarrow f'(x) = f(x) \text{ and } (P^c)^i \equiv f' = f$$

If we recall that relational composition of neutrals corresponded to the intersection of the components of state they kept fixed, then the requirement that n^i and $(n^c)^i$ keep disjoint parts of the restricted state fixed is expressed in the following definition.

A neutral *n respects inv* if $n^i(n^c)^i = inv \times inv$

The fact that $nn^c = W\times W$ means that it is possible to get from any state in the invariant to any other through some intermediate state, possibly one which does not satisfy the invariant. Making n respect the invariant is to insist that the intermediate state is in the invariant. For example, given any two functions from A to A we could find a relation such that we could get from the first function to the relation under R (or P) and then from the relation to the second function under R^c (or P^c). But in the case of R we could always choose the intermediate relation to be a function, this is not in general possible for P.

In the composite $R^i(R^c)^i, (R^c)^i \equiv \forall x \neq a . f'(x) = f(x)$ permits $f(a)$ to change and then $R^i \equiv f'(a) = f(a)$ permits $f(x)$ to change if $x \neq a$. Thus whatever the original value of $f, f1$ say, it is possible under the composite to obtain any other functional value, $f2$ say, afterwards. We simply take an intermediate function which agrees with $f1$ at all points other than a and agrees with $f2$ on a.

Whereas if $f3$ were any intermediate function in a transition from $f1$ to $f2$ under PP^c and if $f1(c) = c$ for some c then since P^c keeps $\{(x,y)\in f \mid x \neq y\}$ fixed we could not have $(c,d)\in f3$, where $c \neq d$, thus $f3(c) = c$ and then, since P keeps $\{(x,y)\in f \mid x = y\}$ fixed, we must have $f2(c) = c$. Thus if for some $c, f1(c) = c$ and $f2(c) \neq c$ then $(f1, f2) \notin P^i(P)^i$ and so in general $P^i(P)^i \neq \text{inv} \times \text{inv}$.

[2] These identities suppose that the notation $f(a)$ on the right-hand side imposes the condition $f\colon A \to A$ etc.

The following result guarantees that the set of all neutrals in a relational boolean algebra which respect a specific invariant will itself form a relational boolean algebra, a "sub relational boolean algebra" of the original one.

Proposition 7.1. If n and m respect *inv* then so do n^c, nm and $n \cap m$.

Proof. If n respects *inv* then $n^i(n^c)^i = inv \times inv$ so if α and β are two elements of *inv* there is a third element, γ, of *inv* such that $\alpha n \gamma$ and $\gamma n^c \beta$, but n and n^c are both symmetric thus we have $\beta n^c \gamma$ and $\gamma n \alpha$ and thus $\beta(n^i(n^c)^i)\,\alpha$. Thus $(n^c)^i n^i = inv \times inv$ so n^c respects *inv*.

Let n and m respect *inv*, thus we have

$$n^i(n^c)^i = inv \times inv \text{ and } m^i(m^c)^i = inv \times inv$$

Then

$$\begin{aligned}(nm^i)^i((nm)^c)^i &= (nm)^i(n^c \cap m^c)^i \\ &= (nm)^i((n^c)^i \cap (m^c)^i) \\ &= (((nm)^i(n^c)^i) \cap ((nm)^i(m^c)^i)) \\ &\supseteq ((n^i(n^c)^i) \cap (m^i(m^c)^i)) && \text{(by R4)} \\ &= ((inv \times inv) \cap (inv \times inv)) \\ &= inv \times inv\end{aligned}$$

But

$$(nm)^i((nm)^c)^i \subseteq inv \times inv$$

Thus nm respects *inv*.

If n and m respect *inv*, then n and m^c respect *inv*, by the first part. Thus by the second part so does $n^c m^c$. One more application of the first part yields, $(n^c m^c)^c = n \cap m$ respects *inv*. □

We now prove the result that if a neutral, for example R above, preserves the specified postcondition, $f'(a) = b$ in the example, and respects the invariant, $f \in A \to A$ in the example, then R^c is central to the augmented event, $f \in A \to A \wedge f'(a) = b \wedge f' \in A \to A$, which insists on re-establishing the invariant.

Proposition 7.2. If n^c preserves an event e and n (or equivalently n^c) respects *inv* then n is central to e^i.

Proof. As for Proposition 4.3. Let n be such that n^c preserves an event e and n respects *inv* and let m be consistent with e.

As shown in Figure 20, we take α in $dom(e^i) = dom(e^i \cap m)$ and thus obtain β in *inv* such that $\alpha e^i \beta$ and $\alpha m \beta$. Since $n^i(n^c)^i = inv \times inv$ we have a δ in *inv* such that $\beta n^c \delta$ and $\alpha n \delta$.

Then since n^c preserves e and α, β are both in *inv*, we have $\alpha e^i \delta$. The result follows using $m = n^c m \cap nm$ as in Proposition 4.3. □

We are able now to redefine *implicitly central* in the case where we have an invariant, *i*. If n^c preserves an event e and n^c respects *inv* then n is termed implicitly central to e^i.

In this section we have considered specifications with an invariant. An invariant is specified, which all states are required to satisfy. An event is then specified with the implicit assumption that the invariant will hold before and afterwards. Thus we specify $f'(a) = b$ in the presence of the invariant $f \in A \to A$ instead of $f \in A \to A \wedge f'(a) = b \wedge f' \in A \to A$. We wish to augment the event by neutral relations. To show that a neutral relation R is central to the combined event it is sufficient to show that it

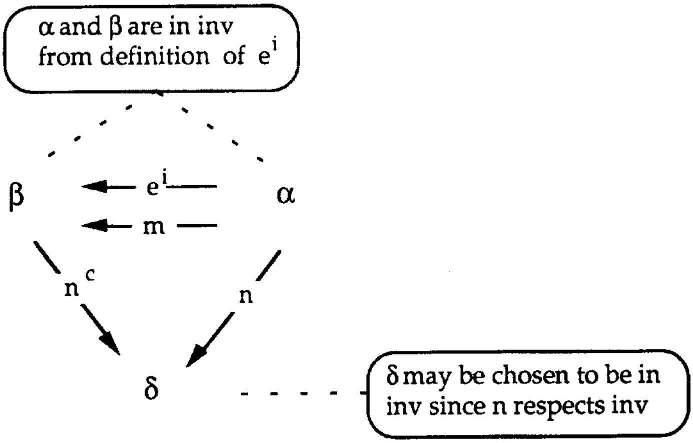

α and β are in inv from definition of e^i
β
e^i
m
α
n^c
n
δ
δ may be chosen to be in inv since n respects inv

Fig. 20

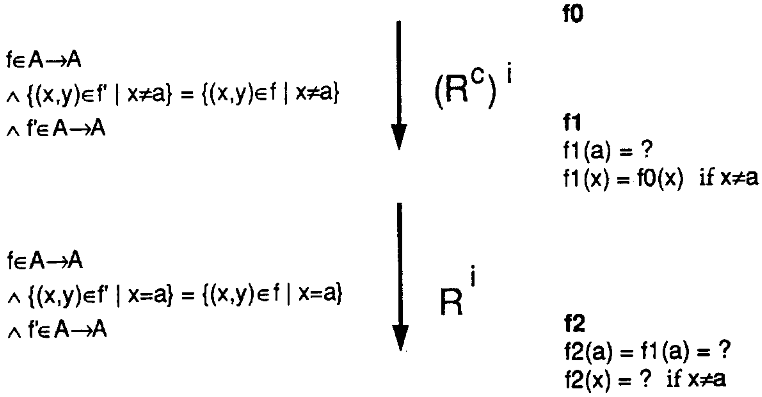


Fig. 21

preserves $f'(a) = b$ and respects $f \in A \to A$. Consider Fig. 21. For any functions $f0$, $f2$: $A \to A$ we have $f0(R^i(R^c)^i)f2$. Thus

$$R \equiv \{(x,y) \in f' \mid x = a\} = \{(x,y) \in f \mid x = a\} \text{ respects the invariant, } f \in A \to A$$

and

$$R \equiv \{(x,y) \in f' \mid x = a\} = \{(x,y) \in f \mid x = a\} \text{ preserves } f'(a) = b$$

Whence $R^c \equiv \{(x,y) \in f' \mid x \neq a\} = \{(x,y) \in f \mid x \neq a\}$ is central to $f \in A \to A \wedge f'(a) = b \wedge f' \in A \to A$ and the augmented specification is

$$f \in A \to A \wedge f'(a) = b \wedge f' \in A \to A \wedge \{(x,y) \in f' \mid x \neq a\} = \{(x,y) \in f \mid x \neq a\}$$

This corresponds to a "functional over-writing" statement in Z. How much easier simply to state $f'(a) = b$.

We are still only augmenting our events by neutrals which are central to them. We now have two simple ways of obtaining such central relations.

8. Relations Implicitly Central to Combined Events (in the Presence of an Invariant)

Since by Proposition 7.1 the set of neutrals which respect the invariant is closed under the boolean algebra operations, we have the analogues of Lemma 5.1 and Proposition 5.2.

Lemma 8.1. If n and m respect *inv* and preserve e and f respectively then $n \cap m$ respects *inv* and preserves $e \cap f$.

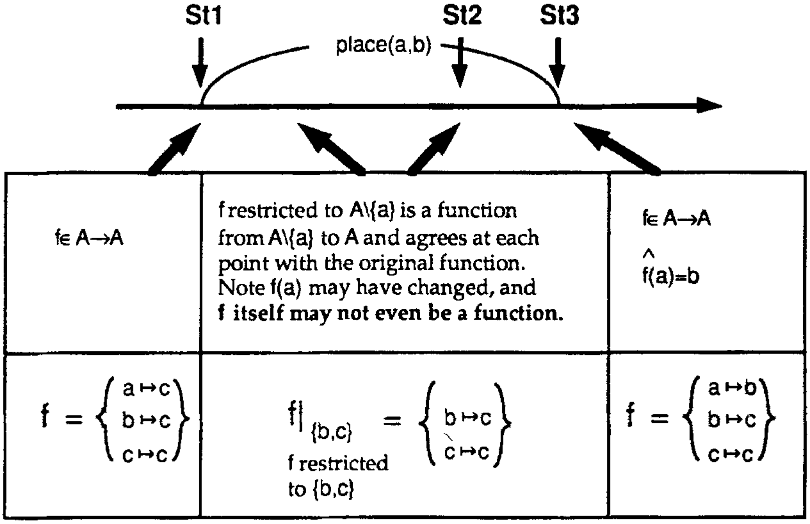
Proposition 8.2. In the presence of an invariant, *inv*, if n_1 and n_2 are implicitly central to e_1 and e_2 respectively, then $n_1 n_2$ is implicitly central to $e_1 \cap e_2$.

Given Proposition 7.1 both proofs follow those of the previous results and are consequently omitted.

9. Reasoning About Concurrent Behaviour

As before we wish to consider events with duration and what we may infer about the state before, during and after the event. We again suggest that if *St*1 is the state at the start of an event, e, then *St*2 is a possible intermediate state just in case *St*1 and *St*2 are related by every relation which is implicitly central to that event. The state on termination of the event, *St*3, is any possible intermediate state which is also related to *St*1 by $e \cap (inv \times inv)$.

For example suppose we have a component of state f: $A \to A$ which is declared to be a function from A to A, and the event place (a, b) specified by $f'(a) = b$. The explicit postcondition is intended to be $(f'(a) = b) \wedge ((f \in A \to A) \wedge (f' \in A \to A))$. The neutral $n_a \equiv \{(x,y) \in f' \mid x \neq a\} = \{(x,y) \in f \mid x \neq a\}$ is implicitly central to this event (Fig. 22).



$f \in A \to A$	f restricted to A\{a} is a function from A\{a} to A and agrees at each point with the original function. Note f(a) may have changed, and **f itself may not even be a function.**	$f \in A \to A$ $\wedge$ $f(a)=b$
$f = \left\{ \begin{matrix} a \mapsto c \\ b \mapsto c \\ c \mapsto c \end{matrix} \right\}$	$f\|_{\{b,c\}} = \left\{ \begin{matrix} b \mapsto c \\ c \mapsto c \end{matrix} \right\}$ f restricted to {b,c}	$f = \left\{ \begin{matrix} a \mapsto b \\ b \mapsto c \\ c \mapsto c \end{matrix} \right\}$

Fig. 22

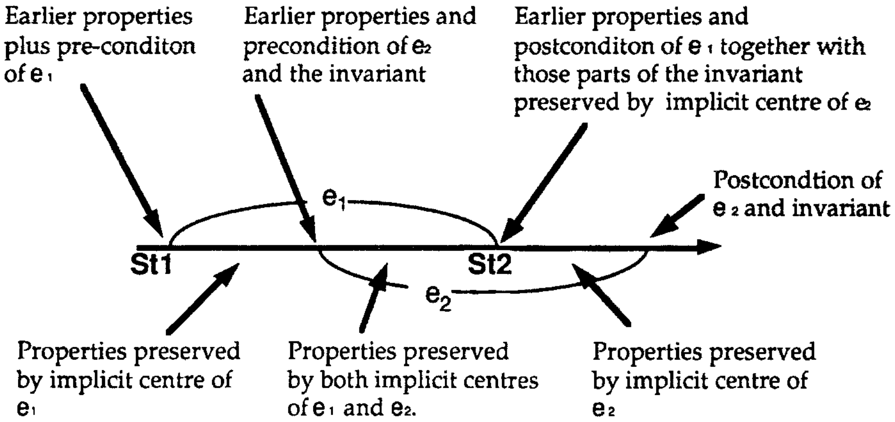

Earlier properties plus pre-conditon of e₁
Earlier properties and precondition of e₂ and the invariant
Earlier properties and postconditon of e₁ together with those parts of the invariant preserved by implicit centre of e₂
Postcondtion of e₂ and invariant
e₁
St1
St2
e₂
Properties preserved by implicit centre of e₁
Properties preserved by both implicit centres of e₁ and e₂.
Properties preserved by implicit centre of e₂

Fig. 23

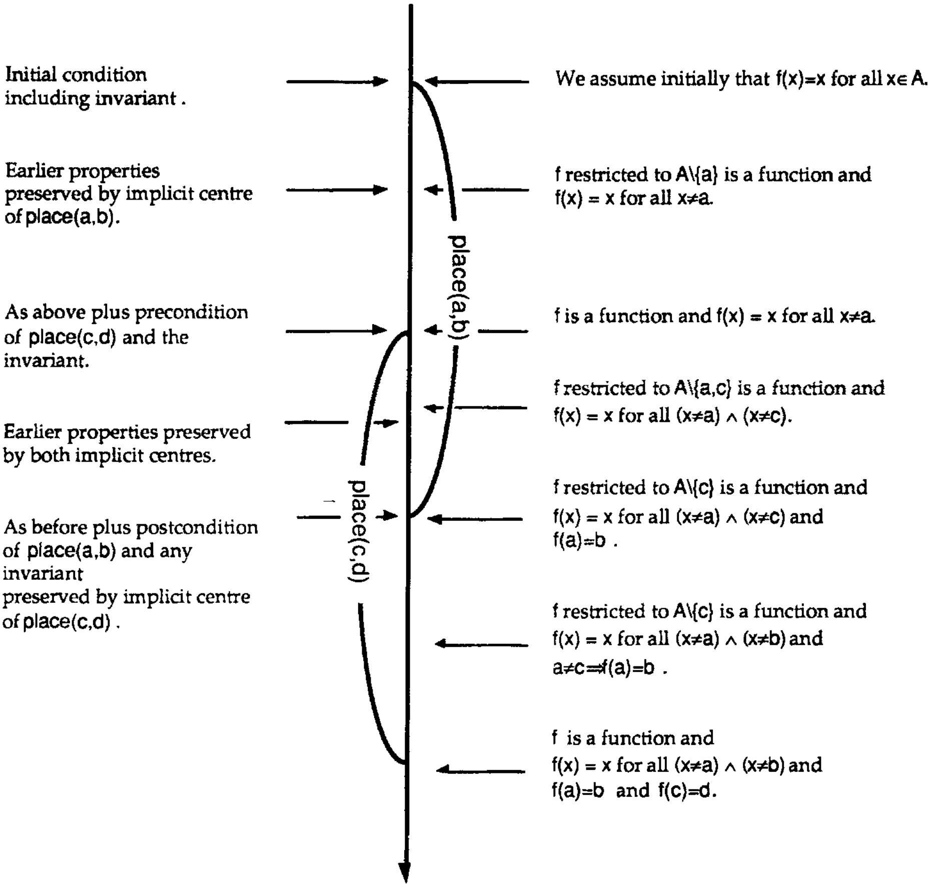

Initial condition including invariant.
We assume initially that f(x)=x for all x∈A.
Earlier properties preserved by implicit centre of place(a,b).
f restricted to A\{a} is a function and f(x) = x for all x≠a.
place(a,b)
As above plus precondition of place(c,d) and the invariant.
f is a function and f(x) = x for all x≠a.
f restricted to A\{a,c} is a function and f(x) = x for all (x≠a) ∧ (x≠c).
Earlier properties preserved by both implicit centres.
f restricted to A\{c} is a function and f(x) = x for all (x≠a) ∧ (x≠c) and f(a)=b .
place(c,d)
As before plus postcondition of place(a,b) and any invariant preserved by implicit centre of place(c,d).
f restricted to A\{c} is a function and f(x) = x for all (x≠a) ∧ (x≠b) and a≠c⇒f(a)=b .
f is a function and f(x) = x for all (x≠a) ∧ (x≠b) and f(a)=b and f(c)=d.

Fig. 24

Notice we do not infer that the intermediate states satisfy the invariant, except insofar as it is preserved by the implicit centrals. Thus if on the termination of one event others are still active we may not be able to guarantee that the whole invariant holds, only that part of it which is not being interfered with by the active events. These conventions are illustrated in Fig. 23. In stating that *St*2 satisfies those parts of the invariant preserved by the implicit centre of e_2 in Fig. 23 we mean tht *St*1 will be related to *St*2 by $(inv \times inv)\,n$ for every neutral n which is implicitly central to e_2.

If events $e_2, e_3, \ldots, e_n$ were still active on the termination of e_1 then *St*1 will be related to *St*2 by $(inv \times inv)\,n_2 n_3 n_r$ for every composition $n_2 n_3 n_r$ of relations n_m, each of which is implicitly central to the orresponding e_m.

As an example consider the case where e_1 is $place(a, b) \equiv (f'(a) = b)$ and e_2 is $place(c, d) \equiv (f'(c) = d)$ with $inv \equiv f \in A \to A$ (Figure 24). Then

$$n_a \equiv \{(x, y) \in f' \mid x \neq a\} = \{(x, y) \in f \mid x \neq a\}$$

and

$$n_b \equiv \{(x, y) \in f' \mid x \neq c\} = \{(x, y) \in f \mid x \neq c\}$$

are implicitly central to e_1 and e_2 respectively. Then

$$(inv \times inv)\,n_b \equiv (f \in A \to A) \wedge (\{x, y) \in f' \mid x \neq a\} \in A \backslash \{a\} \to A))$$

is satisfied by two states precisely if the first satisfies the invariant and f restricted to $A \backslash \{a\}$ is a function to A in the second.

10. Further Work and Conclusion

Finally, one more example is considered involving a state with components A, B, C declared to be a sets of natural numbers, with invariant $A \cap B = C$. Define an event by $e \equiv 1 \in A'$. Then

$$n \equiv (A \backslash \{1\} = A' \backslash \{1\}) \wedge (B \backslash \{1\} = B' \backslash \{1\}) \wedge (C \backslash \{1\} = C' \backslash \{1\})$$

is implicitly central to e by the rules given in Section 7. (Notice that n and n^c respect the invariant.) Note that we are unable to infer whether or not 1 is an element of either B or C after the event, only that if it is in one of them then it is in the other. It may be that the specifier had intended C to be secondary to A and B in some way and that they should be changed, or left alone, first and then C should be modified accordingly. With such a convention the above event would be completely determined and we would be able to make the additional inferences that $(B' = B) \wedge (C' = C \cup (\{1\} \cap B))$. The idea of introducing a priority ordering over the neutral relations and the consequences of such orderings is the subject of ongoing research. It should be noted that the introduction of an invariant corresponded to a class of sub-relational boolean algebras, and the proofs of the principal results in Sections 7 to 9 were simplified by this observation. It will transpire that the introduction of priorities will correspond to the construction of a class of quotient algebras.

The relationship between the relational boolean algebra model and other models of concurrency has been studied by Shields [Shi91a, 91b] and is the subject of further research with reference to the use of more explicitly behavioural specifications, incorporating time, with the object oriented style of [SPB90].

The abstraction of relational boolean algebras has been used to simplify the use, in practical examples, of "rest stays unchanged" event specifications. The main advantage of such specifications is not only that they make the specifier's job simpler in that he or she has less to write, or that the reader of such a specification is presented with an easier specification to understand, but lies in the possibility of a context sensitive interpretation of event specifications. The rest need only stay the same unless another event is interfering with it. This was exploited in Sections 6 and 9 and has been used in specifying a signalling protocol for British Railways and reasoning about the behaviour of the system specified [ByW92].

References

[ByW92] Byers, P. J. and Wilkinson, M. K.: *Formal Safety of Slow Scan SSI.* Commercial Report for B.R., Smith System Engineering Ltd., 1992.

[DaP90] Davey, B. A. and Priestly, H. A.: *Introduction to Lattices and Order.* Cambridge Mathematical Textbooks, 1990.

[DiF88] Dijkstra, E. W. and Feijen, W. H. J.: *A Method of Programming.* Addison-Wesley (1988).

[EVD89] vanEijk, P. H. J., Vissers, C. A. and Diaz, M. (eds): *The Formal Description Technique LOTOS.* North-Holland 1989.

[Hoa85] Hoare, C. A. R.: *Communicating Sequential Processes.* Prentice Hall International, 1985.

[Jon83] Jones, C. B.: Tentative Steps Towards a Development Method for Interfering Programs. *ACM, Transactions on Programming Languages and Systems,* 5 (4) (1983).

[Jon86] Jones, C. B.: *Systematic Software Development Using V.D.M.* Prentice Hall International, 1986.

[Mil89] Milner, R.: *Communication and Concurrency.* Prentice Hall International, 1989.

[ScP86] Schumann, S. A. and Pitt, D. H.: Object Oriented Subsystem Specification. In L. G. T. Meertens (ed.), *Program Specification and Transformation.* North Holland, 1986.

[SPB90] Schuman, S. A., Pitt, D. H. and Byers, P. J.: Object Oriented Process Specification. University of Surrey, Computing Sciences, Technical Report CS-90-01, 1990.

[Shi91a] Shields, M. W.: Let Sleeping DatATypeS Lie. University of Surrey, Computing Sciences, Technical Reports, CS-91-08, 1991.

[Shi91b] Shields, M. W.: Asynchronous Operational Semantics for Abstract Objects, University of Surrey, Computing Sciences, Technical Report, CS-91-09, 1991.

[Spi89] Spivey, J. M.: *The Z Notation.* Prentice Hall International, 1989.

[WoD88] Woodcock, J. C. P. and Dickinson, B.: Using V.D.M. with Rely and Guarantee Conditions: Experiences From a Real Project. In *Proc. VDM Symposium 88,* LNCS 328, Springer-Verlag, 1988.

Received June 1992
Accepted in revised form September 1993 by D. J. Cooke