Some properties of the relative ~~complement~~ converse.

C. A. R. Hoare

March 1995.

Summary. To extend the applicability of the relational calculus to reactive systems, it is necessary to replace the converse operator by a relative converse. This note explores some simple ways of restoring some of the power of the calculus. The presentation is lightened by a series of diagrams, which ensure independence of the properties, and give a sense of coherence, if not completeness to the study.

Let T be a ternary relation over S.

We can define the following operations on subsets of S.

$$P;Q = \{r \mid \exists p,q : p \in P \;\&\; q \in Q : T(p,q,r)\}$$

$$P\backslash R = \{q \mid \exists p,r : p \in P \;\&\; r \in R : T(p,q,r)\}$$

$$R/Q = \{p \mid \exists q,r : q \in Q \;\&\; r \in R : T(p,q,r)\}$$

These definitions already give ~~the~~ ~~of~~ analogues of the standard Schroeder equivalences of the relational calculus (where $P\backslash R = \breve{P};R = (\breve{P}/\breve{R})^{\smile}$)

$$(P;Q) \cap R = \emptyset \quad \text{iff} \quad (P\backslash R) \cap Q = \emptyset$$

$$\text{iff} \quad (R/Q) \cap P = \emptyset.$$

What properties of T are needed to reestablish other interesting theorems in the relational calculus? This brief note explores six independent properties, and gives them a graphical interpretation.

$\cancel{I(a,b,c)}$

The following interpretations of T may be considered of interest in Computing Science

1. S is pairs of machine states, before and after execution of a program. T describes sequential composition

$$T(a,b,c) = (\vec{a} = \overleftarrow{b} \;\&\; \overleftarrow{c} = \overleftarrow{a} \;\&\; \vec{c} = \vec{b})$$

where $\overleftarrow{x}$ and $\vec{x}$ are the left and right components of x.

2. S is pairs of machine states, interpreted as functions from variables to values. T represents parallel composition of disjoint programs.

$$T(a,b,c) = (\overleftarrow{c} = \overleftarrow{a} \oplus \overleftarrow{b} \;\&\; \vec{c} = \vec{a} \oplus \vec{b})$$

where $\oplus$ is union of disjoint functions. (T is false if the functions are not disjoint).

3. S is the set of sequences from some alphabet

$$T(a,b,c) = (a^\frown b = c)$$

representing concatenation of sequences.

4. T represents the CSP definition of parallel composition of traces:

$$T(a,b,c) = (c \in (A \cup B)^* \ \& \ c \upharpoonright A = a \ \& \ c \upharpoonright B = b)$$

where $x \upharpoonright Y$ is x ~~with all l~~ after removal of all letters outside Y.

5. T represents ~~inter~~ CSP interleaving $|||$

$T(a,b,c)$ = c is an interleaving of a and b.

6. T represents CCS interleaving. This is similar to the above, except that ~~adjacent~~ an adjacent pair, consisting of input ~~by one~~ in one string and output from another, may be replaced by τ.

7. S is a set with preorder $\leq$, and

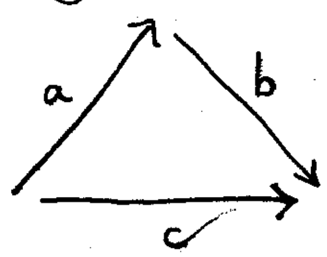
7(a) $T(a,b,c) = (a \leq c)$

or (b) $T(a,b,c) = (b \leq c)$

or (c) $T(a,b,c) = (a \leq b \leq c)$

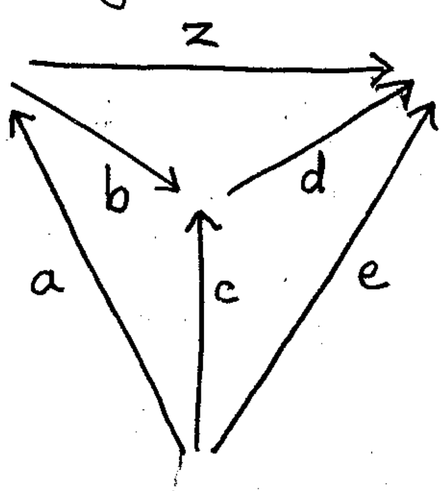
or (d) $T(a,b,c) = (a \leq \cancel{b} \ \& \ b \leq c)$

The proposition $T(a,b,c)$ may be drawn as a triangle, with an acyclic direction ascribed to the edges:



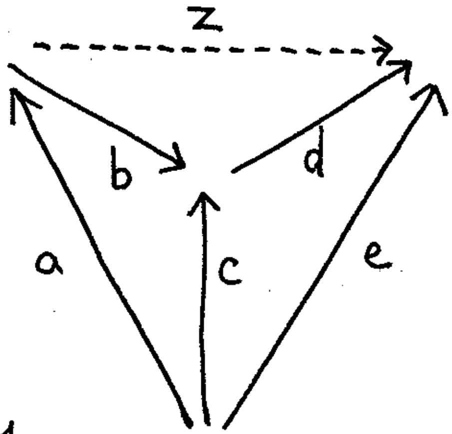
The directions determine the allocation of the labels to the edges, in the order shown.

The conjunction of several such propositions may be drawn as a collection of such triangles, sharing edges with the same label and direction:



$$T(a,b,c) \,\&\, T(c,d,e) \,\&\, T(a,z,e) \,\&\, T(b,d,z)$$

A diagram with a dotted line stands for an implication. The antecedent is extracted by reading the diagram without the dotted line; the consequent is extracted by reading only the triangles involving the dotted line, and this line is existentially quantified:



Axiom 1.

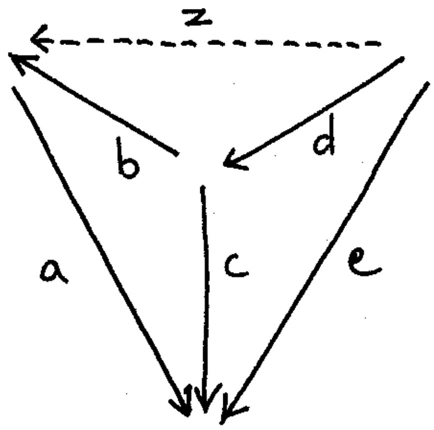
$$T(a,b,c) \,\&\, T(c,d,e) \Rightarrow \exists z :: T(a,z,e) \,\&\, T(b,d,z).$$

This is an interesting property, because it immediately gives one half of the associative law for composition:

$$(A;B);D \subseteq A;(B;D)$$

Proof. $e \in LHS \Rightarrow \exists\, a,b,c,d : a \in A \,\&\, b \in B \,\&\, c \in C \,\&\, d \in D :$
$$T(a,b,c) \,\&\, T(c,d,e)$$
$\Rightarrow \exists\, a,b,d\, z : a \in A \,\&\, b \in B \,\&\, d \in D :$
$$T(a,z,e) \,\&\, T(b,d,z).$$

The dual of a diagram is obtained by reversing all its arrows. The previous diagram is dualised thus:



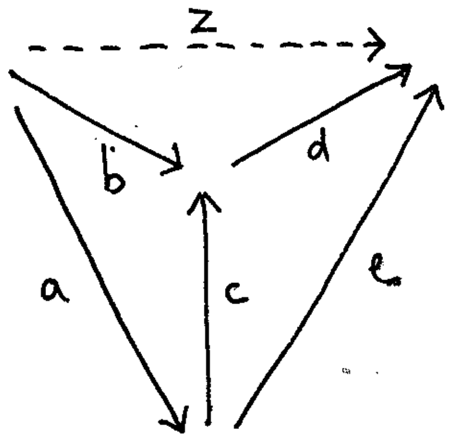
Axiom 2.

This immediately gives the other half of the associative law:

$$D;(B;A) \subseteq (D;B);A$$

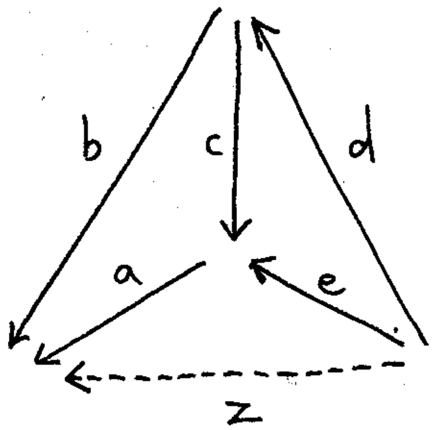
Proof: $e \in LHS \Rightarrow e \in RHS$

A diagram can be self-dual, for example:



Axiom 3.

After reversing the arrows, redraw the diagram so that z is at the bottom:



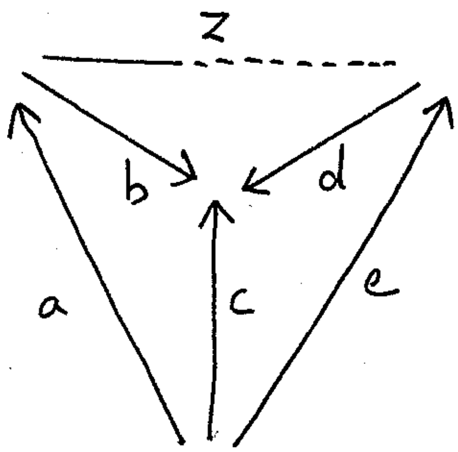
This is just a 180% rotation of the ~~dual~~ original, and so has exactly the same meaning.
But the real interest of the diagram is that it gives two more laws, (and their analogues with \ in place of /):

$$A;(E/D) \subseteq (A;E)/D$$

$$B/(E/D) \subseteq (B;D)/E$$

In the relational calculus, these are both equations.

Often ~~When~~ the validity of a diagram is unaffected by changing the direction of an arrow, provided that the result is non-cyclic; such an arrow can be left undirected. For example, in the previous diagram, the arrow c could have been drawn without a direction, because it does not matter. The arrow z could also be undirected, because there is only one consistent way of giving it a direction. In general, a diagram with undirected arrows is read as a disjunction of all consistent ways of ascribing directions to them; as shown in the following diagram



Axiom 4.

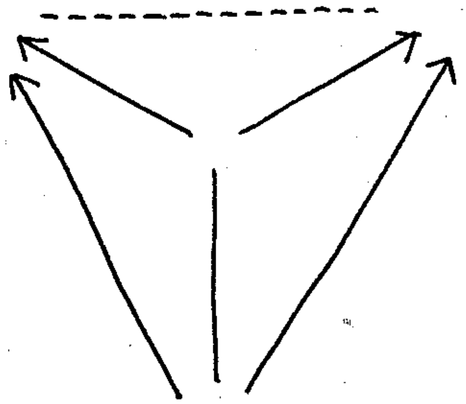
$$T(e,d,c) \,\&\, T(a,b,c) \Rightarrow \exists z :: T(e,z,a) \,\&\, T(z,b,d)$$
$$\vee\ T(a,z,e) \,\&\, T(z,d,b)$$

This diagram is clearly self-dual. More amazing, it establishes an inclusion in the reverse direction to those of the previous diagram

$$(E;D)/B \subseteq E;(D/B) \cup E/(B/D)$$

The same holds with \ in place of /.

One great advantage of diagrams is that the edges do not have to be labelled



Axiom 5.

The corresponding theorem, like its predecessors, requires three variables:

$$(E/D);B \subseteq E/(B\backslash D) \cup E;(D\backslash B)$$

This is trivial in the relational calculus, where all three terms are equal to

$$E;\breve{D};B$$

The dual diagram gives rise to

$$B;(D\backslash E) \subseteq (D/B)\backslash E \cup (B/D);E$$

Axiom 6

All our diagrams consist of solid lines of two triangles sharing a single edge. There are only $\frac{3 \times 4}{2} = 6$ different ways of drawing such a figure, and we have drawn all of them. The conjunction of all the diagrams can be drawn very conveniently as a single tetrahedron with all the edges undirected: ~~in summary~~, this states that any non-cyclic ascription of directions to any five of the edges can be noncyclically extended to the sixth edge.

But we are also interested in predicates T which satisfy some of the ~~six~~ six diagrams and not others. There exist predicates which satisfy any five of the diagrams, but fail to satisfy just one. Consider the predicate which is true only of the solid lines in the omitted diagram. Because the dotted line of this diagram is absent, ~~it f~~ the diagram is not satisfied. But all the five ~~six other~~ remaining diagrams are trivially satisfied, because their antecedents do not match those of the omitted law, The diagrammatic method of this little note is due to Sharon Curtis and Gavin Lowe; and the theorems are due to Burghard von Karger.

C. A. R. Hoare

March 1995.