Tony,

Congratulations.

What you have done is to get the original types of proof I was attempting using the conjugate algebras to work.

Your simplification in observing that $a^{\boxed{a}} = 1$ is at the same level as my simplification in moving from the conjugate to the box algebra. It is that which allows this proof to work, since we no longer have to worry about the different places our last messages get re-absorbed.

You have eliminated Peirced arcs from the proof, which means that one no longer extracts from the proof either the existence or the value of the algebraic invariant I use. Thus I think both proofs have independent interest.

BM

Bill Roscoe

About consistency in databases.

If we extend the definition of $a^{[b]}$ (page 34) to include $a^{[a]} = I$ if $a = b$, * then we can avoid treating absorption of a message as a special case. We then have only two rules

1. $[v, I] \to [(v;u), u], u$

The processor with current accumulated update v and empty E spontaneously generates update u, and sends it as a message to the right

2. $x, [v, e] \to [v; x^{[e]}, e^{[x]}], x^{[e]}$

The processor inputs x on the left, outputs $x^{[e]}$ on the right, and changes its state accordingly. In the case $x = e$, this gives

$$e.[v, e] \to [v; I, I], I,$$

and we can easily ignore identity messages.

---

* I haven't checked that P1, P2, and P3 are still true.

Now suppose a link between two processors contains two messages $m2, m1$. I claim that these may be merged into a single message $(m1; m2)$, without affecting the ultimate result. This may increase efficiency in practice and simplify proofs in the theory. Consider the fragment

$$m2, m1, [v, e] \text{ ---all the other processes}$$

$$\to m2, [v; m1^{\boxed{e}}, e^{\boxed{m1}}], m1^{\boxed{e}} \qquad \text{after one step}$$

$$\to \left[v; m1^{\boxed{e}}; m2^{\boxed{e^{\boxed{m1}}}}, \left(e^{\boxed{m1}}\right)^{\boxed{m2}}\right], m2^{\boxed{e^{\boxed{m1}}}}, m1^{\boxed{e}} \quad (*)$$

The messages will necessarily be absorbed by the remaining processes; therefore, by induction, their order can be reversed without affecting the outcome, giving

$$m1^{\boxed{e}}; m2^{\boxed{e^{\boxed{m1}}}} \underset{P2}{=} (m1; m2)^{\boxed{e}}$$

Using P3 as well,

$$(*) = \left[v; (m1; m2)^{\boxed{e}}, e^{\boxed{m1; m2}}\right], (m1; m2)^{\square}$$

But this is exactly the same as the effect of $(m1; m2), [v, e]$.

Yesterday I proved a congruence theorem permitting combination of adjacent messages, passing through a process that does not fire.

if $m2, m1\,[v,e] \longrightarrow [w,f]\,n2, n1$

then $(m1;m2)[v,e] \longrightarrow [w,f](n1;n2)$

Original to Bill Rounds 5/7

Today I prove an analogous theorem combining a pair of adjacent processes that have already fired

Define ";" by $[v,e];[w,f] \triangleq [w, e;f]$

$[v,I] \to [v,I],[(v;u),u]\,u$ (4/4, 2e)

Thm. If $m\,[v,e]\,[w,f] \longrightarrow [v',e']\,[w',f']\,m'$

then $m([v,e];[w,f]) \longrightarrow ([v',e'];[w',f'])\,m'$

Proof: $m\,[v,e]\,[w,f]$

$\to [v; m^{[e]}, e^{[m]}]\; m^{[e]}\,[w,f]$

$\to [v; m^{[e]}, e^{[m]}]\; [w; (m^{[e]})^{[f]}, f^{[m^{[e]}]}]\; (m^{[e]})^{[f]}$ *

But $m([v,e];[w,f]) = m\,[w,(e;f)]$

$\to [w; m^{[e;f]}, (e;f)^{[m]}]\; m^{[e;f]}$

$= [w; (m^{[e]})^{[f]}, (e^{[m]}; f^{[m^{[e]}]})]\; (m^{[e]})^{[f]}$ [by P2, P3

$= ([w; m^{[e]}, e^{[m]}]; [w; (m^{[e]})^{[f]}, f^{[m^{[e]}]}])\,(m^{[e]})^{[f]}$ [by def

* Since fired processes are deterministic, these uniquely define the values of (v', e', w', f', m')

consider a non-firing process, after all other processes have fired. Since R is deterministic, we let it fire until all messages m are accumulated to the left of $[v, I]$. Amalgamate them to m.

Now consider the case that $[v, I]$ never fires:

$$m\,[v, I]\,R \;\to\; [v; m, I]\,m\,R.$$

By induction on the number of firing processes, mR goes to the target state S with all machines equal to $[v; m, I]$

Now consider the case that $[v, I]$ fires with message u

$$m\,[v; u, u]\,u\,R$$

$$\to [v; u; m^{u}, u^{m}]\; m^{u}\; u\; R \qquad *$$

but $m^{u}\,u = u; m^{u} = m; u^{m} = u^{m}, m$

$$S_0\,* \longrightarrow [v; m; u^{m}, u^{m}]\; u^{m}\; S$$

$$\to u^{m}\,[v; m; u^{m}, u^{m}]\; S'$$

where all the values of S' are $v; m; u^{m}$

$$\to [v; m; u^{m}, I]\; S'$$

QED.