Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

P. Urzyczyn

Dining philosophers and process algebra

Computer Science/Department of Software Technology Note CS-N8603 March

The Centre for Mathematics and Computer Science is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

Dining Philosophers and Process Algebra

Pawel Urzyczyn
Institute of Mathematics
University of Warsaw
PKIN
00-901 Warszawa, Poland

We discuss a liveness property for merges of regular processes, and we apply this property to show correctness of a dining philosophers protocol by means of process algebra.

Key words and phrases: process algebra, dining philosophers, liveness, fairness, probabilistic fairness, fair abstraction.
Note: This research was done during a visit to CWI in september 1985. Partial support was obtained from Esprit project 432, Meteor.
69F11, 69F12, 69F32, 69F43

INTRODUCTION

In this paper we are concerned in merges $X\|Y$ of regular processes X, Y defined by systems of linear equations of the form

$$X = X_1$$

$$X_i = a_{i1}X_1 + \cdots + a_{iM}X_M$$

(and similarly for Y). Assuming that H is the set of communicating actions, and I denotes the set of all actions except those proper for X, we consider the following condition

$$\tau\cdot\tau_I\circ\partial_H(X\|Y) = \tau\cdot\tau_I(X) \tag{0.1}$$

which we call *liveness of X within* $\partial_H(X\|Y)$. The intuitive meaning of (0.1) is that the right-hand side describes the proper behaviour of process X when considered separately from any "outside world", while the left-hand side is the proper behaviour of X within the merge, in the environment determined by process Y, both modulo "silent" τ-steps. In general, the environment may restrict the possible behaviour of X. Thus, (0.1) states that it is not the case, i.e. that the proper behaviour of X remains unchanged even if X has to coorperate with Y.

A quite natural, stronger version of (0.1) may be obtained by replacing everywhere X by X_i and Y by Y_j and adding a universal quantifier ranging over all $\partial_H(X_i\|Y_j)$ which are accessible from $\partial_H(X\|Y) = \partial_H(X_1\|Y_1)$ by means of sequences of atomic actions. This condition will be called *uniform liveness of X in* $\partial_H(X\|Y)$.

Below we give a necessary and sufficient condition on the merge $\partial_H(X\|Y)$ for the uniform liveness of X (Theorem 2.6.), and prove that uniform liveness implies deadlock-freedom of $\partial_H(X\|Y)$ under a simple assumption on X (Prop. 1.12.). As an example, we consider a well-known protocol for the dining philosophers problem, expressed in process algebra, and prove the liveness condition for this protocol.

In what follows, we make a strong use of Cluster Fair Abstraction Rule (CFAR), introduced recently by F. Vaandrager, which is a generalization of the following Koomen's Fair Abstraction Rule (KFAR):

$$KFAR\frac{X = iX + Y,\ i\in I}{\tau_I(X) = \tau\cdot\tau_I(Y)}\ .$$

Note CS-N8603
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

It occurs however, that the liveness property is not sufficient to imply correctness of protocols like those for dining philosophers. Namely, the equation (0.1), and also its uniform version, does not exclude behaviours of $\partial_H(X \| Y)$ in which no proper actions of X do occur. We obtain (0.1) since CFAR abstracts from these behaviours, making no difference between the following two situations:

1. X does not perform any proper action (a philosopher does not eat), since it does not perform any action at all;
2. X performs only communicating actions, and this communication work is not efficient, since it does not lead to any proper action (a philosopher takes a fork, puts it back, takes another fork, and so on).

Thus, except the liveness condition, we have to consider also a kind of fairness condition. The one we propose is the following

$$\partial_{\alpha(x)} \circ \tau_{I'} \circ \partial_H(X_i \| Y_j) = t_{ij} \cdot \delta \tag{0.2}$$

for some closed term t_{ij}, where $\alpha(X)$ is the alphabet of X, and $I' = \alpha(Y)$. We prove that the protocol for dining philosophers with semaphore does satisfy (0.2), for all accessible $\partial_H(X_i \| Y_j)$, while another live protocol does not.

However it may be also said that the liveness condition guarantees a kind of probablistic fairness, no matter if (0.2) holds or not (Prop. 4.12.).

The paper is arranged as follows. In section 1, we introduce some definitions, and consider some basic properties of liveness. Section 2 is devoted to prove the necessary and sufficient condition for uniform liveness. The protocol for dining philosophers with semaphore is considered in section 3, and the fairness issues are discussed in section 4.

§1. Preliminaries

1.1. This paper is not intended to be self-contained, and assumes that the reader is familiar with the ACP$_\tau$ system, as described in [BK1], [BK3] and [BK4]. Below we give only definitions of the specific notions used in paper, and explain some non-standard use of terminology.

We are concerned here with regular processes only, i.e. processes that can be defined by finite systems of guarded linear equations, as defined in [BK3]. Throughout the paper, we restrict ourselves to consider systems of equations of the form

$$X_i = a_{i1}X_1 + \cdots a_{iM}X_M \quad (\textit{for } i = 1, \ldots, M) \tag{1.1.1}$$

1.2. To be precise, we should note the difference between a process and its specification. The capitals $X_1, \ldots, X_M$ above denote *variables* in a specification, and we should use another notation, say $x_1, \ldots, x_M$ for a solution of the system (1.1.1). However, by the Recursive Specification Principle (see 1.13.2), such a solution is always unique, and in fact it belongs to the algebra of regular processes (see [BK3]). On the other hand, it will be always clear from the context what is the specification assigned to a process under consideration. Thus we do not state this distinction explicitly, and we will use the same notation for processes and the corresponding variables.

1.3. It is always assumed that in (1.1.1.) all $a_{ij} \in a \cup \{\delta\}$, for $i, j, \leqslant M$, but we require at least one component on the right-hand side to be nontrivial, i.e. we assume $\forall i \exists j (a_{ij} \neq \delta)$. We usually skip the condition $a_{ij} \neq \delta$, when referring to a_{ij}. Thus, e.g. "$a_{ij} \notin H$" means "$a_{ij} \notin H \cup \{\delta\}$".

For simplicity we assume that all the variables X_i are different. The reader may easily observe that any system of equations (1.1.1) may be transformed, by introducing new variables, so that it satisfies this condition, and the process X_1 it defines, does not change (see also 1.11). The process X_1 is the one we are usually interested in, and we denote it also by X.

1.4. The processes X_i occurring in the system of equations (1.1.1.) are called *states* of the process X. We say that a state X_j is *accessible* from another state X_i *in one step* (*one B-step,* for a certain $B \subseteq A$) iff $a_{ij} \neq \delta$ ($a_{ij} \in B$). We denote this fact by $X_j \leftarrow X_i$ ($X_j \overset{B}{\leftarrow} X_i$). *Accessible* will mean the transitive and reflexive closure of accessible in one step, and we will say that X_i *is accessible* iff it is accessible from X_1. We use the notation $\twoheadleftarrow$ ($\overset{B}{\twoheadleftarrow}$) for accessibility. Clearly $\twoheadleftarrow\!\!\!\twoheadrightarrow$ ($\overset{B}{\twoheadleftarrow\!\!\!\twoheadrightarrow}$) is an equivalence relation, and $\twoheadleftarrow$ ($\overset{B}{\twoheadleftarrow}$) becomes a (finite, thus well-founded) partial order on the equivalence classes of $\twoheadleftarrow\!\!\!\twoheadrightarrow$ ($\overset{B}{\twoheadleftarrow\!\!\!\twoheadrightarrow}$).

The *alphabet* of X, denoted $\alpha(X)$ is defined by

$$\alpha(X) = \{a_{mn} : X_m \twoheadleftarrow X_1 \wedge a_{mn} \neq \delta \wedge a_{mn} \neq \tau\}$$

Note that this definition is equivalent to that given in [BBK1].

1.5. A process X is said to be *cyclic* iff every equation (1.1.1.) contains only one non-trivial summand at the right-hand side. We will use the informal notation

$$X_i = \alpha_i \cdot X_{i+1}$$

for cyclic processes.

1.6. Suppose that X and Y are two processes given by systems of linear equations as above. It is a routine to verify that $X \| Y$, $\partial_H(X \| Y)$, $\tau_I \circ \partial_H(X \| Y)$, etc. can be also presented by systems of linear equations, possibly not satisfying the condition that the right-hand sides are always different from δ (In the latter case there may be also coefficients equal to τ). Usually we will need this observation for $\partial_H(X \| Y)$, and in this case we will have to ensure that $\partial_H(X \| Y)$ is *deadlock-free,* i.e. for accessible $\partial_H(X_i \| Y_j)$ we have $\partial_H(X_i \| Y_j) \neq \delta$. (We extend our terminology concerning states, accessibility, etc. for merges (encapsulated and abstracted merges). Clearly, states of e.g. $\partial_H(X \| Y)$ have the form $\partial_H(X_i \| Y_j)$ for X_i, Y_j being respectively states of X and Y).

1.7. In case a merge $X \| Y$ is considered we say that an action $a \in A$ is *proper* for X iff $a \in \alpha(X)$ and it is not a communicating action, i.e. $(a|b) = \delta$, for all $b \in \alpha(Y)$. An action $a \in A$ is *allowed* for a state X_i of X iff there is a j such that $a = a_{ij}$. For the encapsulated merge $\partial_H(X_i \| Y_j)$ we say that $a \in \alpha(X)$ is allowed iff it is allowed for X_i and either it is proper for X or there is a $b \in \alpha(Y)$, allowed for Y_j such that $(a|b) \neq \delta$. That is, allowed actions are those which can be actually performed.

1.8. From now on, H will always mean the set of communicating actions, i.e.

$$H = \{a \in \alpha(X) : \exists b \in \alpha(Y) : (a|b) \neq \delta\} \cup \{b \in \alpha(Y) : \exists a \in \alpha(X) : (a|b) \neq \delta\}$$

The symbol $H|H$ denotes the set of results of communications:

$$H|H = \{(a|b) : a,\ b \in H\}$$

We also assume that $I = \alpha(Y) \cup H \cup (H|H)$ and that $|I| \geqslant 2$.

1.9. We say that X is *live* in the encapsulated merge $\partial_H(X \| Y)$ iff

$$\tau \cdot \tau_I \circ \partial_H(X \| Y) = \tau \cdot \tau_I(X)$$

X is *uniformly live* in $\partial_H(X \| Y)$ iff, for all accessible states $\partial_H(X_i \| Y_j)$ of $\partial_H(X \| Y)$ it holds that

$$\tau \cdot \tau_I \circ \partial_H(X_i \| Y_j) = \tau \cdot \tau_I(X_i)$$

1.10. REMARK In fact it is the case that $\tau_I \circ \partial_H(X_i \| Y_j)$ is either $\tau_I(X_i)$, or $\tau \cdot \tau_I(X_i)$ (see 2.7. and 2.12.), but the above condition is much more convenient.

1.11. We need one more assumption about our systems of equations. Namely, we assume that each equivalence class of $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$ may be considered to be a *cluster* in the sense of [V], that is

$$\text{if } X_m \overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow} X_n \text{ then } a_{mn} \in I \cup \{\delta\}$$

Observe that is not an essential restriction. Indeed, let E denote the system of equations for X, and suppose that there is an $a_{mn} \notin I$ with $X_m \overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow} X_n$. For each such a_{mn} we introduce a new variable X_n^m and replace X_n by X_n^m in the equation defining X_m. Then we add a new equation $X_n^m = RHS_n$, where RHS_n is the right-hand side of the equation defining X_n in E. This way we obtain a new specification E', where the "wrong" a_{mn}'s do not cause any trouble, since X_n^m is now not a member of the class of X_m. Also, the equivalence class of X_n^m is one-element, since X_n^m may be accessed only from X_m by an action not in I. Thus, no new "wrong" coefficient appear in E'. Clearly, E' is equivalent to E extended with the equations $X_{mn} = X_n$. This means that our restriction on systems of equations does not restrict the class of processes they define.

Observe also that if the system of equations for X does satisfy the above condition then so does the system defining $X \| Y$. Indeed, if $(X_m \| Y_n) \overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow} (X_k \| Y_l)$ and a is an atom that leads from $(X_m \| Y_n)$ to $(X_k \| Y_l)$ then either it is a member of $\alpha(Y) \cup (H|H) \subseteq I$ or it has the form $a_{mn} \in I$.

1.12. Let C be a subset of an equivalence class of $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$. Consider the relation $\overset{I}{\longrightarrow}$ restricted to members of C, and the equivalence relation determined by its reflexive transitive closure. If this relation is total on C (there is only one equivalence class) then we say that C is a *cluster* in the system of equations for X.

1.13. Let us consider now a list of additional axioms we use together with ACP$_\tau$. All of these axioms were proved to hold for the algebra of regular processes, except 1.13.1 which is an assumption about the language rather than an axiom.

1.13.1. Handshaking Axiom

$$a|b|c = \delta \quad \text{for all } a,\ b,\ c \in A$$

1.13.2. Recursive Specification Principle (see [BK2])
if $\overline{Z} = (Z_1, \ldots, Z_m)$ *and* $\overline{V} = (V_1, \ldots, V_m)$ *are solutions of the same system of guarded equations, then* $\overline{Z} = \overline{V}$ (For our purposes, we may define a *guarded* equation to be of the form (1.1.1) with all $a_{ij} \neq \tau$, or to be obtained from (1.1.1) by replacing its right-hand side, RHS, with the expression $\tau \cdot$ RHS. For the general definition see [BK2]).

1.13.3. Conditional Axioms (see [BBK1])

$$\text{(CA1)} \qquad \frac{\alpha(X) | (\alpha(Y) \cap H) \subseteq H}{\partial_H(X \| Y) = \partial_H(X \| \partial_H(Y))}$$

$$\text{(CA5)} \qquad \frac{H' \cup H'' = H}{\partial_H(X) = \partial_{H'} \circ \partial_{H''}(X)}$$

1.13.4. Some assumptions about the processes δ and $\tau\delta$
We accept the following four axioms for all processes x,y and any atom $a \neq \delta$:
a) $\tau x = \tau\delta \rightarrow x = \delta \vee x = \tau\delta$;
b) $x + y = \tau\delta \rightarrow x = \tau\delta \vee x = \delta$;
c) $x + y = \delta \rightarrow x = \delta$;
d) $ax \neq \delta$, $ax \neq \tau\delta$ and $\tau\delta \neq \delta$.
The reader may easily check that all them hold for regular processes using the fact (see [BKO]) that there are only five regular processes in which no atom except δ does occur. These processes are $\tau(\tau + \tau\delta)$, $\tau + \tau\delta$, $\tau\delta$, τ and δ, and all of them are different.

1.13.5. Cluster fair abstraction rule.
Let X be given by a system of equations of the form (1.1.1) and let C be a cluster containing X_i. Then for all $X_j \in C$ it holds that

$$\tau \cdot \tau_I(X_j) = \tau \cdot (\sum_{\substack{m \in c \\ n \notin c}} \tau_I(a_{mn}) \cdot \tau_I(X_n))$$

If the sum above is empty we consider it to be equal to δ.
(The above is a simplified and slightly adopted version of the original formulation. It is left to the reader to check that 1.13.5 does indeed follow from CFAR. Pay attention to the case when the equivalence class contains only one element.)

As an application of CFAR we show the following proposition, which also demonstrates the inductive technique used later for lemma 2.9.

1.14. PROPOSITION *If X is uniformly live in $\partial_H(X \| Y)$ and for each accessible X_i there is an X_j, accessible from X_i which allows a step not in I, then $\partial_H(X \| Y)$ is deadlock-free.*

PROOF: By the uniform liveness it suffices to prove that for all accessible X_i, $\tau \cdot \tau_I(X_i) \neq \tau\delta$. Indeed, this implies $\tau \cdot \tau_I \circ \partial_H(X_i \| Y_j) \neq \tau\delta$, whence $\partial_H(X_i \| Y_j) \neq \delta$.

We prove the claim $\tau \cdot \tau_I(X_i) \neq \tau\delta$ by an induction on equivalence classes of $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$ with respect to the partial ordering $\overset{I}{\twoheadleftarrow}$. Suppose that for some accessible X_i,.

$$\tau \cdot \tau_I(X_i) = \tau\delta$$

Denote by C the equivalence class of $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$ determined by X_i. By CFAR, we have

$$\tau\delta = \tau \cdot \tau_I(X_i) = \tau \cdot (\sum_{\substack{m \in C \\ n \notin C}} \tau_I(a_{mn}) \circ \tau_I(X_n))$$

Using the axioms in 1.13.4, we conclude that all the summands $\tau_I(a_{mn}) \circ \tau_I(X_n)$ are either δ or $\tau\delta$. If all are equal to δ then C consists of all states accessible from X_i, and because of 1.11 no step outside of I is allowed for any of them. Thus, there is $n \notin C$ with $\tau_I(a_{mn}) \circ \tau_I(X_n) = \tau\delta$, in which case $a_{mn} \in I$, by 1.13.4 and we obtain $\tau \cdot \tau_I(X_n) = \tau\delta$. But $X_n \notin C$ and is I-accessible from X_i and this allows us to apply the inductive hypothesis $\tau \cdot \tau_I(X_n) \neq \tau\delta$ which contradicts the above.

§2 Liveness of a regular process in a merge

2.1. Throughout this Section we assume that $X = X_1$ and $Y = Y_1$ are regular processes defined by systems of equations

$$E_X : X_i = T_i(\overline{X}) \quad \text{for } i \leqslant M,$$

$$E_Y : Y_j = S_j(\overline{Y}) \quad \text{for } j \leqslant N,$$

where $\overline{X}$ $(\overline{Y})$ denotes the vector of variables $X_1, \ldots, X_M$ $(Y_1, \ldots, Y_N)$, and

$$T_i(\overline{X}) = a_{i1}X_1 + \cdots + a_{iM}X_M$$

$$S_j(\overline{Y}) = b_{j1}Y_1 + \cdots + b_{jN}Y_N$$

We assume all the conventions and assumptions about systems of equations as stated in Section 1. In addition, we will assume that all the sets: $\alpha(X)-H$, $\alpha(Y)-H$, $\alpha(X)\cap H$, $\alpha(Y)\cap H$ and $H|H$ are disjoint, where H is the set of communicating actions as in 1.8. Recall also that $I = \alpha(Y) \cup H \cup (H|H)$.

2.2. Consider the encapsulated-merge $\partial_H(X \| Y)$. We will say that X is *locally live* in $\partial_H(X\|Y)$ iff the following condition holds:

2.2.1. Suppose that $\partial_H(X_i \| Y_j)$ is an accessible state of $\partial_H(X\|Y)$. Then for any $a_{ik} \in H$ there exist m,n,k' such that

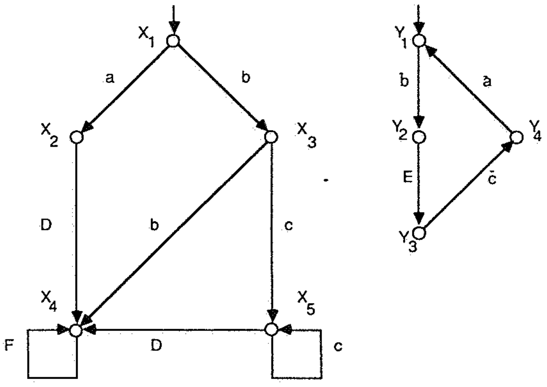
1) $\partial_H(X_m \| Y_n) \overset{I}{\twoheadleftarrow} \partial_H(X_i \| Y_j)$;
2) $X_{k'} \overset{I}{\twoheadleftarrow} X_m$;
3) if $X_k \notin [X_i]$ then $\partial_H(X_m \| Y_n) \notin [\partial_H(X_i \| Y_j)]$
4) $\tau \cdot \tau_I(X_{k'}) = \tau \cdot \tau_I(X_k)$

2.3. The condition 2.2.1 seems to require a little explanation. It would be simpler to consider e.g. the following condition: *if X_i and Y_j are as above then, after a (possibly empty) sequence of I-steps, a state $\partial_H(X_i \| Y_l)$ may be reached from $\partial_H(X_i \| Y_j)$ so that the action a_{ik} is allowed in $\partial_H(X_i \| Y_l)$.* That is, if X_i is ready to execute a_{ik}, then it has a chance to do so, no matter what is the context it occurs in within the merge. The condition 2.2.1 is a weakened version of the above. First we do not require that a_{ik} has to be executed at all, but only a process $X_{k'}$ satisfying (4) above has to be reached in I-steps. Second, these I-steps do not have to be performed in $\partial_H(X\|Y)$, it is enough if only an initial sequence of them is legal in $\partial_H(X\|Y)$, up to the first step leading outside of $[\partial_H(X_i \| Y_j)]$. Then it suffices to have the rest of the sequence only potentially allowed, i.e. allowed in X.

2.4. As an example consider the following situation:

$$\begin{array}{ll}
X_1 = aX_2 + bX_3 & \qquad Y_1 = \bar{b}Y_2 \\
X_2 = DX_4 & \qquad Y_2 = EY_3 \\
X_3 = cX_5 + bX_4 & \qquad Y_3 = \bar{c}Y_4 \\
X_4 = FX_4 & \qquad Y_4 = \bar{a}Y_1 \\
X_5 = DX_4 + cX_5 &
\end{array}$$

where $(a|\bar{a}) = A$, $(b|\bar{b}) = B$, $(c|\bar{c}) = C$ and there is no other communication. The processes X and Y are presented on the following picture:



Then the condition 2.2.1 is satisfied for $\partial_H(X_1 \| Y_1)$, since $\partial_H(X_3 \| Y_2) \xleftarrow{I} \partial_H(X_1 \| Y_1)$ and $X_5 \twoheadleftarrow^{I} X_3$ and $\tau \cdot \tau_I(X_5) = \tau \cdot \tau_I(DX_4) = \tau \cdot D \cdot \tau(X_4) = \ \tau \cdot \tau_I(X_2)$, by KFAR. However it is not satisfied by $\partial_H(X_3 \| Y_3)$ since the only action to perform here is $C = (c|\overline{c})$ and then we get to $\partial_H(X_5 \| Y_4)$. But no process X_k satisfying $\tau \cdot \tau_I(X_k) = \tau \cdot \tau_I(X_4) = \tau \cdot F^{\omega}$ is accessible from X_5.

2.5. Note that if X is cyclic the condition 2.2.1 takes the form *If $\partial_H(X_i \| Y_j)$ is accessible and $a_i \| Y_j)$ is accessible and $a_i \in H$, then $\partial_H(X_{i+1} \| Y_l)$ is, for some l, accessible from $\partial_H(X_i \| Y_j)$ in I steps.*
In other words: the action a_i has to be eventually allowed, after a (possibly empty) sequence of proper Y-steps.

2.6. THEOREM *Let X, Y be as above. Then X is locally live in $\partial_H(X \| Y)$ if and only if it is uniformly live in $\partial_H(X \| Y)$.*

PROOF: The implication from left to right will follow from lemma 2.9 below by an application of the Recursive Specification Principle. For the other direction observe that $\tau \cdot \tau_I(X_i) = \ \tau \cdot \tau_I \circ \partial_H(X_i \| Y_j)$ implies that the graphs $\tau_I(X_i)$ and $\tau_I \circ \partial_H(X_i \| Y_j)$ are equivalent w.r.t. (possibly not rooted) τ-bisimulation (see [BK3]). Let now $a_{ik} \notin H$.. This means that $\tau_I(X_k)$ is accessible from $\tau_I(X_i)$ by a τ-step. By the bisimilarity there is a node $\tau_I \circ \partial_H(X_m \| Y_n)$ accessible from $\tau_I \circ \partial_H(X_i \| Y_j)$ by τ-steps, and such that the corresponding subtrees are τ-bisimilar. Hence $\tau \cdot \tau_I(X_k)$ is $r\tau$-bisimilar to $\tau \cdot \tau_I \circ \partial_H(X_m \| Y_n) = \tau \cdot \tau_I(X_m)$. The reader can easily check that 2.2.1 is thus satisfied.

2.7. REMARK The uniform liveness in fact implies the condition mentioned in 2.3. Also it means in fact that $\tau_I \circ \partial_H(X_i \| Y_j)$ is either $\tau_I(X_i)$ or $\tau \cdot \tau_I(X_i)$. For this assume first that some $\partial_H(X_i \| Y_l)$ is accessible from $\partial_H(X_i \| Y_j)$ in one I-step. Then, for some Z, $\tau_I \circ \partial_H(X_i \| Y_j) = \ \tau \cdot \tau_I \circ \partial_H(X_i \| Y_l) + Z = \tau \cdot \tau_I(X_i) + Z = \ \tau \cdot \tau_I \partial_H(X_i \| Y_j) + Z$. But the implication $x = \tau x + y \rightarrow x = \tau x$ holds for all x,y. Indeed, $\tau x = \ \tau(\tau x + y) = \ \tau(\tau x + y) + \tau x + y = \ \tau x + \tau x + y = \ \tau x + y = x$. Thus $\tau \cdot \tau_I \circ \partial_H(X_i \| Y_j) = \tau_I \circ \partial_H(X_i \| Y_j)$. The equation $\tau_I \circ \partial_H(X_i \| Y_j) = \ \tau_I(X_i)$ will hold provided X_i is accessible from itself in at least one I-step. The remaining case is considered in Remark 2.12.

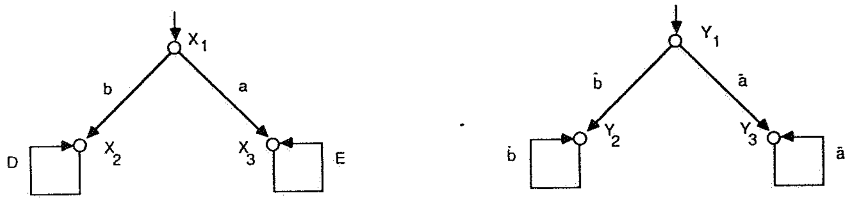
2.8. REMARK It is easily seen that the local liveness is *not* a necessary condition for liveness (non-uniform). The condition

$$\tau \cdot \tau_I(X) = \tau \cdot \tau_I \circ \partial_H(X \| Y)$$

does not imply

$$\tau \cdot \tau_I(X_i) = \tau \cdot \tau_I \circ \partial_H(X_i \| Y_j) \quad \text{for all} X_i, \ Y_j$$

since it may happen that $\tau_I\circ\partial_H(X_i\|Y_j)\neq\tau_I\circ\partial_H(X_i\|Y_i)$. As a counterexample one can consider processes described by the following picture



Here $(a|\bar{a})=A$,$(b|\bar{b})=B$, other communications give δ.
Clearly, $\tau\cdot\tau_I(X_1)=\tau\cdot\tau_I\circ\partial_H(X_1\|Y_1)=\tau(\tau D^\omega+\tau E^\omega)$, but $\tau\cdot\tau_I\circ\partial_H(X_1\|Y_2)=\tau D^\omega\neq\tau\cdot\tau_I(X_1)$.

2.9. LEMMA *Let X, Y be as in Theorem 2.6. Then, for all accessible $\partial_H(X_i\|Y_j)$, there is a guarded equation*

$$E_{ij}:Z_{ij}=T_{ij}(\bar{Z})$$

(where $\bar{Z}$ denotes the variables $Z_{k,l}$ for $k\leqslant M$, $l\leqslant N$) satisfied by

$$Z_{k,l}=\tau\cdot\tau_I\circ\partial_H(X_k\|Y_l)\quad\text{for } k\leqslant M,\ l\leqslant N,$$

and also by

$$Z_{k,l}=\tau\cdot\tau_I(X_k)\quad\text{for } k\leqslant M,\ l\leqslant N.$$

For the proof of Lemma 2.9 we need the following simple observation:

2.10. LEMMA *If X_m is accessible from X_k in I-steps, then*

$$\tau\cdot\tau_I(X_k)=\tau\cdot\tau_I(X_k)+\tau\cdot\tau_I(X_m).$$

PROOF: goes by induction on the number of I-steps. Suppose that $X_m\overset{I}{\leftarrow}X_i\overset{I}{\twoheadleftarrow}X_k$, and apply the induction hypothesis for X_i (Using the ACP$_\tau$-law : $\tau(x+y)+y=\tau(x+y)$):

$$\begin{aligned}\tau\cdot\tau_I(X_k)&=\tau\cdot\tau_I(X_k)+\tau\cdot\tau_I(X_i)=\\&=\tau\cdot\tau_I(X_k)+\tau(\sum_{a_{il}\notin H}a_{il}\cdot\tau_I(X_l)+\sum_{\substack{a_{il}\in H\\ l\neq m}}\tau\cdot\tau_I(X_l)+\tau\cdot\tau_I(X_m))=\\&=\tau\cdot\tau_I(X_k)+\tau\cdot\tau_I(X_i)+\tau\cdot\tau_I(X_m)=\\&=\tau\cdot\tau_I(X_k)+\tau\cdot\tau_I(X_m)\end{aligned}$$

2.11. Proof of Lemma 2.9:

The proof goes by induction on the equivalence classes of the relation $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$ defined on the states of $\partial_H(X\|Y)$. For $i\leqslant M, j\leqslant N$, let $[\partial_H(X_i\|Y_j)]$ denote the equivalence class determined by $\partial_H(X_i\|Y_j)$.

Assume the inductive hypothesis for all $\partial_H(X_k\|Y_l)\notin[\partial_H(X_i\|Y_j)]$ such that $\partial_H(X_k\|Y_l)\overset{I}{\twoheadleftarrow}\partial_H(X_i\|Y_j)$. By the Cluster Fair Abstraction Rule applied to the equations

$$\partial_H(X_m \| Y_n) = \sum_{a_{mk} \notin H} a_{mk} \cdot \partial_H(X_k \| Y_n) + \sum_{b_{nl} \notin H} b_{nl} \cdot \partial_H(X_m \| Y_l) + \sum_{(a_{mk}|b_{nl}) \neq \delta} (a_{mk}|b_{nl}) \cdot \partial_H(X_k \| Y_l)$$

we obtain

$$\tau \cdot \tau_I \circ \partial_H(X_i \| Y_j) = \tau(\sum_{\substack{(m,n)\in C \\ a_{mk} \notin H}} a_{mk} \cdot \tau_I \circ \partial_H(X_k \| Y_n) + \sum_{\substack{(m,n)\in C \\ (k,l)\notin C \\ (a_{mk}|b_{nl})\neq\delta}} \tau \cdot \tau_I \circ \partial_H(X_k \| Y_l) + \sum_{\substack{(m,n)\in C \\ (m,l)\notin C \\ b_{nl}\notin H}} \tau \cdot \tau_I \circ \partial_H(X_m \| Y_l)),$$

where $C = \{(m,n) : \partial_H(X_m \| Y_n) \in [\partial_H(X_i \| Y_j)]\}$. The equation E_{ij} will have the form

$$Z_{ij} = \tau(\sum_{\substack{(m,n)\in C \\ a_{mk} \notin H}} a_{mk} \cdot Z_{kn} + \sum_{\substack{(m,n)\in C \\ (k,l)\notin C \\ (a_{mk}|b_{nl})\neq\delta}} \tau \cdot RHS_{k,l} + \sum_{\substack{(m,n)\in C \\ (m,l)\notin C \\ b_{nl}\notin H}} \tau \cdot RHS_{m,l})$$

where $\mathrm{RHS}_{p,q}$, for $(p,q)\notin C$, denotes the right-hand side of the equation $E_{p,q}$, which existence follows by the induction hypothesis.

The reader may easily check that it is enough to prove that

$$\tau \cdot \tau_I(X_i) = RHS$$

where

$$RHS = \tau(\sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3)$$

and

$$\sum\nolimits_1 = \sum_{\substack{m\in S \\ a_{mk}\notin H}} a_{mk} \cdot \tau_I(X_k)$$

$$\sum\nolimits_2 = \sum_{k\in B} \tau \cdot \tau_I(X_k)$$

$$\sum\nolimits_3 = \sum_{m\in E} \tau \cdot \tau_I(X_m)$$

and

$$S = \{m \leqslant M : \exists n \leqslant N((m,n)\in C)\}$$

$$B = \bigcup_{m\leqslant N} B_m$$

$$B_m = \{k \leqslant M : \exists n,l((m,n)\in C, (k,l)\notin C, (a_{mk}|b_{nl})\neq\delta)\}$$

$$E = \{m \leqslant M : \exists n,l((m,n)\in C, (m,l)\notin C, b_{n,l}\notin H)\}$$

Now observe that the set $\{X_m : m\in S\}$ forms a cluster (in the sense of 1.12). Indeed, if $m_1,m_2\in S$ then $(m_1,n_1)\in C$ and $(m_2,n_2)\in C$, for some n_1,n_2, and thus $\partial_H(X_{m_1} \| Y_{n_1} \overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow} \partial_H(X_{m_2} \| Y_{n_2})$. Removing the proper steps of Y, we obtain $X_{m_1} \overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow} X_{m_2}$. Thus we see that $\{X_m : m\in S\}$ is a subset of the $\overset{I}{\twoheadleftarrow\!\!\twoheadrightarrow}$s-equivalence class of X_i and that the I-accessibility within S is achieved with use of elements of S only. Thus, using CFAR, we can conclude that:

$$\tau \cdot \tau_I(X_i) = \tau(\sum\nolimits_1 + \sum\nolimits_{II})$$

where

$$\sum\nolimits_{II} = \sum_{k\in D} \tau \cdot \tau_I(X_k)$$

and

$$D = \{k \notin S : \exists m \in S(a_{mk} \in H)\}$$

Note that $E \subseteq S$, and $B, D \subseteq \{k : \exists m \in S(a_{mk} \in H)\}$.
We have to prove $\tau(\sum_1 + \sum_2 + \sum_3) = \tau(\sum_1 + \sum_{II})$. This is done by cases.
Case 1:Assume that $\sum_3 \neq \delta$, i.e. $E \neq \varnothing$. Since $E \subseteq S$, we obtain from CFAR, that $\sum_3 = \tau \cdot \tau_I(X_i) = \sum_{m \in s} \tau \cdot \tau_I(X_m)$. Thus, using the axiom: $\tau x + x = \tau x$, we obtain:

$$RHS = \tau(\sum_1 + \sum_2 + \sum_{m \in s} \tau \cdot \tau_I(X_m)) = \tau(\sum_i + \sum_2 + \sum_{m \in s} (\tau \cdot \tau_I(X_m) + \tau_I(X_m))) =$$

$$= \tau(\sum_1 + \sum_2 + \sum_{m \in s} \tau_I(X_m) + \sum_3) =$$

$$= \tau(\sum_1 + \sum_2 + \sum_1 + \sum_{\substack{m \in s \\ a_{mk} \in H}} \tau \cdot \tau_I(X_k) + \sum_3) =$$

$$= \tau(\sum_1 + \sum_{\substack{m \in s \\ a_{mk} \in H}} \tau \cdot \tau_I(X_k) + \sum_3) = \tau(\sum_3) = \tau \cdot \tau \cdot \tau_I(X_i) = \tau \cdot \tau_I(X_i)$$

Case 2:Now let $\sum_3 = \delta$, i.e. $RHS = \tau(\sum_1 + \sum_2)$, and let $k_0 \in B - D$. Then $\exists m \in S(a_{mk_0} \in H)$ but $k_0 \in s$. Thus, $\tau\tau_I(X_{k_0} = \tau \cdot \tau_I(X_i) = \sum_{m \in s} \tau \cdot \tau_I(X_m)$ and we have:

$$RHS = \tau(\sum_1 + \sum_2) = \tau(\sum_1 + \sum_2 + \tau \cdot \tau_I(X_{k_0})) = \tau(\sum_1 + \sum_2 + \tau \cdot \tau_I(X_i))$$

$$= \tau(\sum_1 + \sum_2 + \sum_{m \in S} \tau \cdot \tau_I(X_m)) = \text{ (using the fact that } \tau(x+y) + x = \tau(x+y)) =$$

$$= \tau(\sum_{m \in S} [\tau(\sum_{a_{mk} \notin H} a_{mk} \cdot \tau_I(X_k) + \sum_{a_{mk} \notin H} \tau \cdot \tau_I(X_k)) + \sum_{a_{mk} \notin H} a_{mk} \cdot \tau_I(X_k) + \sum_{k \in B_m} \tau \cdot \tau_I(X_k)]) =$$

$$= \tau(\sum_{m \in S} \tau(\sum_{a_{mk} \notin H} a_{mk} \cdot \tau_I(X_k) + \sum_{a_{mk} \in H} \tau \cdot \tau_I(X_k))) = \tau \cdot \sum_{m \in S} \tau \cdot \tau_I(X_m) = \tau \cdot \tau \cdot \tau_I(X_i) = \tau \cdot \tau_I(X_i)$$

Case 3:Finally assume that $\sum_3 = \delta$ and $B \subseteq D$. We prove

$$\sum_{II} = \sum_2$$

which will immediately imply the hypothesis. For this let $k_0 \in D$, i.e. $k_0 \notin S$ and $\exists m \in S(a_{mk_0} \in H)$. There is an n such that $\partial_H(X_m \| Y_n) \in [\partial_H X_i \| Y_i)]$. By the uniform liveness, there are $\partial_H(X_p \| Y_q) \in [\partial_H(X_i \| Y_j)]$ and $\partial_H(X_k \| Y_l) \notin [\partial_H(X_i \| Y_j)]$, such that $(a_{pk} | b_{ql}) \neq \delta$ and $X_{k_0} \overset{I}{\twoheadleftarrow} X_k$. This means that $k \in B$, and we have $\sum_2 = \sum_2 + \tau \cdot \tau_I(X_k)$. Using lemma 2.10 we get $\sum_2 = \sum_2 + \tau \cdot \tau_I(X_k) + \tau \cdot \tau_I(X_{k_0} = \sum_2 + \tau \cdot \tau_I(X_{k_0}$. Repeating this procedure for all $k_0 \in D - B$, we get $\sum_2 = \sum_{II}$ which completes the proof.

2.12. Remark. We can now complete Remark 2.7. For this observe that if no proper action of Y is allowed in $\partial_H(X_i \| Y_j)$ then we can prove without using CFAR, that $\tau_I \circ \partial_H(X_i \| Y_j) = \tau_I(X_i)$ by comparing the expressions:

$$\tau_I(X_i) = \sum_{a_{ik} \notin H} a_{ik} \cdot \tau_I(X_k) + \sum_{a_{ik} \in H} \tau \cdot \tau_I(X_k)$$

and

$$\tau_I \circ \partial_H(X_i \| Y_j) = \sum_{a_{ik} \notin H} a_{ik} \cdot \tau_I \circ \partial_H(X_k \| Y_j) + \sum_{(a_{ik} | b_{jl}) \neq \delta} \tau \cdot \tau_I \circ \partial_H(X_k \| Y_l) =$$

$$= \sum_{a_{ik} \notin H} a_{ik}\tau_I(X_k) + \sum_{(a_{ik}|b_{jl})\neq\delta} \tau\cdot\tau_I(X_k)$$

by a method similar to that used in Case 3 of the previous proof.

§3. Dining Philosophers

3.1. We describe the dining philosophers protocol (as in [B-A]) by means of process algebra. The philsophers P_i, for $i = 0, \ldots, 4$ are processes defined by recursion equations of the form (indices are taken modulo 5):

$$P_i = T_i \cdot w \cdot f_i^i \cdot f_{i+1}^i \cdot E_i \cdot b_i^i b_{i+1}^i \cdot s \cdot P_i$$

Here T_i denotes "thinking", E_i denotes "eating", and the remaining, auxiliary actions have the following meanings:

f_j^i - take the $j-th$ *fork,*
b_j^i - put the $j-th$ fork *back* on the table,
w - *wait* until the semaphore is greater than zero, allowing the process to enter its critical section,
s - *signal* that the critical section is over.

(We assume that the philosophers and the forks are numbered clockwise, with the i^{th} fork placed to the right of the i^{th} philosopher.)

The semaphore s can take values values in $\{0, \ldots, 4\}$ and is described by a system of equations of the form:

$$\begin{cases} s = s_4 \\ s_4 = d \cdot s_3 \\ s_i = d \cdot s_{i-1} + a \cdot s_{i+1} \quad \text{for } i = 1,2,3 \\ s_0 = a \cdot s_1 \end{cases}$$

(The equation $s = s_4$ may be considered to be informal.) Here, the action d denotes *decreasing* the semaphore by 1, while a is to *add* 1 to the semaphore. Both of them are "potential" actions and may be performed only together with their counterparts from the P_i's, resulting in "actual" actions: $D = (w|d)$ and $A = (s|a)$.

The forks F_i, for $i = 0, \ldots, 4$ are defined by equations:

$$F_i = (t_i^i \cdot r_i^i + t_i^{i-1} \cdot r_i^{i-1}) \cdot F_i$$

where the t_i^j and r_i^j are potential actions, resulting in actual actions $T_i^j = (f_i^j|t_i^j)$, $R_i^j = (b_i^j|r_i^j)$ for the fork being *taken* or *returned*.

The symbol H will denote the set of all communication actions, and I will stand for the set of all actions except T_0 and E_0. Thus, $\tau_I \circ \partial_H(P_0 \| \cdots \| P_4 \| s \| F_0 \| \cdots \| F_4)$ describes the essential behaviour of the philosopher P_0 within the merge. Our goal is to show that

$$\tau_I \circ \partial_H(P_0 \| \cdots \| F_4) = \tau \cdot \tau_I(P_0) = \tau \cdot (T_0 \cdot E_0)^\omega$$

i.e. that the protocol is correct with respect to P_0. By symmetry the same holds for other philosophers.

3.2. We will use the following notation:

$$H' = \{t_1^0,\ r_1^0,\ t_0^0,\ r_0^0,\ d,\ a\}$$

$$H'' = H - H'$$

Thus, H' denotes the set of the communication actions which can communicate with P_0, H'' the set of those which cannot.

$$X = P_0$$

$$Y' = P_1 \| \cdots \| P_4 \| s \| F_0 \| \cdots \| F_4$$

$$Y = \partial_{H''}(Y')$$

Thus, $P_0 \| \cdots \| F_4 = X \| Y'$, and by conditional axioms CA1, CA5 (see [BBK1]) we get

$$\partial_H(X \| Y') = \partial_{H'} \circ \partial_{H''}(X \| Y') = \partial_{H'} \circ \partial_{H''}(X \| \partial_{H''}(Y')) = \partial_H(X \| Y)$$

We are going to apply the results of Section 2 to prove:

$$\tau_I \circ \partial_H(X \| Y) = \tau \cdot \tau_I(X)$$

(Note that the sets I and H above are slightly different then those considered in Section 1, namely they contain some "superfluous" atoms, which do not occur at all in X and $X \| Y$, like e.g. t_1^1. This however does not change the meaning of τ_I and ∂_H.)

3.3. For this we have to show that X and Y satisfy the assumptions in Theorem 2.6. First we observe that the equations defining P_i's and F_i's can be easily transformed into systems of linear equations. It is also easy to obtain a system of linear equations for Y' and Y, and also for $\partial_H(X \| Y)$. Clearly, states of $\partial_H(X \| Y)$ are encapsulations of merges of states of P_0 and states of Y. The latter are encapsulations of merges of states of the other processes. Thus, for each state Q of $\partial_H(X \| Y)$ we can define $Q(P_i)$ ($Q(F_i)$, $Q(s)$) to be the "local" state of P_i (resp. F_i,s) occurring in the "global" state Q in the merge. (Note that the local states determine the global one.)

Since P_i's are cyclic, we can identify for simplicity the states of P_i with their first actions. Thus, e.g. $Q(P_0) = w$ stands for $Q(P_0) = w \cdot f_0^0 \cdot f_1^0 \cdot E_0 \cdot b_0^0 \cdot s \cdot P_0$. For each state Q of $X \| Y$ we define

$$\alpha_Q(i) = \begin{cases} 0 & \text{if } Q(P_i) \in \{P_i, w\} \\ 1 & \text{otherwise} \end{cases}$$

That is, $\alpha_Q(i) = 1$ if P_i is in its critical section. Further, let β_Q denote the number i such that $Q(s) = s_i$.

3.4. Lemma. *A state Q is accessible in $\partial_H(X \| Y)$ iff the following conditions hold:*

3.4.1.) $0 \leqslant \beta_Q = 4 - \sum_{i=0}^{4} \alpha_Q(i) \leqslant 4$

3.4.2.) $Q(F_i) = r_i^i \cdot F_i$ iff $Q(P_i) \in \{f_{i+1}^i, E_i, b_i^i\}$

3.4.3.) $Q(F_{i+1}) = r_{i+1}^i \cdot F_{i+1}$ iff $Q(P_i) \in \{E_i, b_i^i, b_{i+1}^i\}$

Proof: The proof for the direction from left to right goes by induction on the accessibility relation (upside-down). First we prove 3.4.1. For this we see that in the initial state $Q = \partial_H(X \| Y)$ we have $\beta_Q = 4$ and $\alpha_Q(i) = 0$ for all i, since $Q(P_i) = F_i$. Now assume that Q satisfies the induction hypothesis and that Q' is accessible from Q in one step. Clearly, the only actions that may change β_Q or $\alpha_Q(i)$ are the D and A actions, and it is easy to verify that if D is executed, the value of β_Q decreases by 1, while some $\alpha_Q(i)$ increases by 1. Similarly for A. Moreover, if $\beta_Q = 0$, then the action

D is impossible and thus $\beta_{Q'} \geqslant 0$. Similarly, if $\beta_Q = 4$ then $\beta_{Q'} \leqslant 4$.

Now we prove 3.4.2. Clearly, for $Q = \partial_H(X \| Y)$, the hypothesis is obvious. Now let Q satisfy the condition and Q' be accessible form Q in one step (i.e. the appropriate equation has the form $Q = \cdots + cQ' + \cdots$). If c is an action not involving F_i and P_i, then Q' still satisfies 3.4.2. If c is F^i_{i+1} or E_i, both sides of of the condition remain true, if $c \in \{B^i_{i+1}, A, T_i, D\}$, both remain false. Executing F^i_i or B^i_i changes the truth values of both. The proof of 3.4.3 is similar.

We turn to the other implication. For this assume that Q satisfies the invariants 3.4.1 - 3.4.3. Let $n(Q) = \sum_{i=0}^{4} (p_i(Q) + f_i(Q)) + 4 - \beta_Q$ where, for $i = 0, \ldots, 4$,

$$f_i(Q) = \begin{cases} 0 & \text{for } \; Q(F_i) = F_i \\ 1 & \text{for } \; Q(F_i) \in \{r^{i-1}_i \cdot F_i, \; r^i_i \cdot F_i\} \end{cases}$$

$$p_i(Q) = \begin{cases} 0 & \text{for } \; Q(P_i) = P_i \\ j & \text{for } \; Q(P_i) \text{ being the } j^{th} \text{ symbol in the} \\ & \qquad \text{sequence } w, \, f^i_i, \, f^i_{i+1}, \, E_i, \, b^i_i, \, b^i_{i+1}, \, s \end{cases}$$

Clearly, $n(Q) = 0$ iff $Q = \partial_H(X \| Y)$. We claim that if $n(Q) > 0$ then Q is accessible from some Q' with $n(Q') < n(Q)$, which gives an inductive proof of the accessibility of Q.

Suppose that for some i, $p_i(Q) \in \{1,5\}$. Then Q is accessible from the state Q' defined by replacing in Q the local state w (resp. b^i_i) by P_i (resp. E_i). Now $n(Q') = n(Q) - 1$. Now suppose that there is an i with $p_i(Q) \in \{3,4\}$. To obtain Q', we replace $Q(P_i) = f^i_{i+1}$ (resp. E_i) by f^i_i (resp. f^i_{i+1}) and $Q(F_i) = r^i_i$ (see 3.4.2) by F_i (resp. $Q(F_{i+1}) = r^i_{i+1}$ is replaced by $Q'(F_{i+1}) = F_{i+1}$). Clearly, $n(Q') = n(Q) - 2$.

If $p_i(Q) = 6$ for some i, and $Q(F_i) = F_i$ then Q is accessible from Q'' where $p_i(Q) = 5$, and $f_{i(Q)} = 1$. Thus, $n(Q'') = n(Q)$ and Q'' satisfies the first case. If $p_i(Q) = 6$, but $Q(F_i) = r^{i-1}_i \cdot F_i$then $p_{i-1}(Q) \in \{3,4,5\}$, thus satisfying one among the previous cases. Similarly, for $p_i(Q) = 7$, for some i.

The next case is when $p_i(Q) = 2$, for some i. Then $\alpha_Q(i) = 1$, whence $\beta_Q < 4$. We choose Q' to satisfy $Q'(P_{i)} = w$ and $Q'(\dot{s}) = s_{\beta_Q + 1}$. Then $n(Q') = n(Q) - 2$.

The last case to be considered is when $p_i(Q) = 0$ for all i. But then, by the invariants, we see that $Q(F_i) = F_i$ for all forks, and also $\alpha_Q(i) = 0$, for all i, whence $\beta_Q = 4$. Thus, $n(Q) = 0$.

3.5. Lemma. *X is locally live in $\partial_H(X \| Y)$.*

Proof: We will prove that for every accessible state Q, and every $i = 0,\ldots,4$, if $Q(P_i) \in H$ then $Q(P_i)$ is allowed after some sequence of steps not involving the E_i and T_i actions. The hypothesis will follow from 2.5. We inspect the possible cases of $Q(P_i)$.

Case 1.$Q(P_i) = b^i_i$ or b^i_{i+1}. Then $Q(F_i) = r^i_i$ (or resp. $Q(F_{i+1}) = r^i_{i+1}$), by 3.4.1-2, and the communication may be performed immediately.

Case 2.$Q(P_i) = s$. Then $\alpha_Q(i) = 1$ and $\beta_Q \leqslant 3$, whence A may be performed.

Case 3.$Q(P_i) = f^i_i$. If this action is impossible then if must be the case that (see 3.4.3) $Q(F_{i)} = r^{i-1}_i \cdot F_i$. Thus, $Q(P_{i-1}) \in \{E_{i-1}, b^{i-1}_{i-1}, b^{i-1}_i\}$. By Case 1, these actions may be executed, and we get a Q' accessible from Q in τ-steps such that $Q'(P_4) = s$, and $Q'(F_0) = F_0$. Then (since still $Q'(P_i) = f^i_i$), the action F^i_i may be executed.

Case 4.$Q(P_i) = f^i_{i+1}$. Let k be the greatest number number such that for all $j = 0, \ldots, k$ it holds that $Q(P_{i+j}) = f^{i+j}_{i+j+1}$. Clearly, $k \leqslant 3$, otherwise all the processes would visit their critical sections simultaneously. If F^{i+k}_{i+k+1} is not allowed in Q then $Q(F_{i+k+1}) = r^{i+k+1}_{i+k+1}$, whence $Q(P_{i+k+1}) \in \{f^{i+k+1}_{i+k+2}, E_{i+k+1}, b^{i+k+1}_{i+k+1}\}$. The first possibility is excluded, the other two allow sequences of τ-steps ending with some Q' satisfying $Q'(P_{i+k+1}) = b^{i+k+1}_{i+k+2}$, and $Q'(F_{i+k+1} = F_{i+k+1}$. Finally F^{i+k}_{i+k+1} may be executed and we can decrease k by 1. Repeating this argument k times we obtain the possibility of executing F^i_{i+1}.

Case 5.$Q(P_i) = w$. If $\beta_Q > 0$ then D may be performed immediately. Otherwise, the other processes visit their critical sections, and, by cases 1-4 each of them is eventually allowed to execute A, which is increasing β_Q, thus allowing D.

REMARK: We should note that, in all the cases in which we used the induction hypothesis, the obtained sequence of steps cannot involve E_i or T_i, since in all these cases the initial value of $Q(P_i)$ remains unchanged for all states along the sequence.

3.6. COROLLARY.

$$\tau_I \circ \partial_H(P_0 \| \cdots \| P_4 \| F_0 \| \cdots \| F_4 \| s) = \tau \cdot \tau_I(P_0) = \tau(T_i \cdot E_i)^\omega$$

PROOF: immediate from 3.5.

§4. REMARKS ON FAIRNESS

In Sections 2 and 3 we discussed a method of proving a liveness property of parallel computations. The liveness condition we considered, $\tau_I \circ \partial_H(X \| Y) = (\tau)\tau_I(X)$ guarantees that the behaviour of the process X in the merge $X \| Y$ remains unchanged modulo I-steps. This property is however unsatisfactory from some point of view. To see this, consider the following example.

4.1. Suppose that the pilosophers are not obliged to take the right fork first, but that they can non-deterministically choose to take the left one first or the right one first. In addition, a pilosopher can always put the first fork he has taken back on the table (e.g. if he cannot get the second one). Assuming that there is no semaphore, one can describe the new philosopher as follows:

$$P_i = T_i \cdot P'_i$$

$$P'_i = f_i^i \cdot P''_i + f_{i+1}^i \cdot P'''_i$$

$$P''_i = b_i^i \cdot P'_i + f_{i+1}^i \cdot P_i^{iv}$$

$$P'''_i = b_{i+1}^i \cdot P'_i + f_i^i \cdot P_i^{iv}$$

$$P_i^{iv} = E_i \cdot (b_i^i \| b_{i+1}^i) \cdot P_i$$

The behaviour of forks remains unchanged.

4.2. PROPOSITION. *Let P_i be defined as in 4.1. Then each philosopher P_i is uniformly live in the encapsulated merge $\partial_H(P_0 \| \cdots \| P_5 \| F_0 \| \cdots \| F_5)$.*

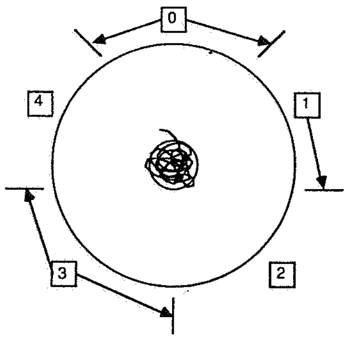
PROOF: (outlined) First we observe that the invariants 3.4.2 and 3.4.3 of lemma 3.4 take now the following form:
(*) $Q(F_i) = r_i^i \cdot F_i$ iff $Q(P_i) \in \{P''_i, P_i^{iv}, (b_i^i \| b_{i+1}^i)P_i, b_i^i \cdot P_i\}$
(**) $Q(F_{i+1}) = r_{i+1}^i \cdot F_{i+1}$ iff $Q(P_i) \in \{P'''_i, P_i^{iv}, (b_i^i \| b_{i+1}^i)P_i, b_{i+1}^i \cdot P_i\}$
Now the proof of liveness is even easier than that of Lemma 3.5. The case of T_i,E_i and b_j^i follow again by the invariants. Suppose then that $Q(P_i) = P'_i$. If P_i cannot perform e.g. f_i^i, then $Q(F_i) = r_i^{i-1} \cdot F_i$. By (*) we see that P_{i-1} can either execute E_i and then b_i^{i-1} or can do b_i^{i-1} immediately. The same holds for f_{i+1}^i. For $Q(P_i) \in \{P''_i, P'''_i\}$ the situation is similar.

Finally, by Theorem 2.6, we conclude that P_i's are all uniformly live.

4.3. We see that the new, simpler, protocol behaves equally well when we abstract from actions in I. However, there is something wrong with it, namely, there is a possibility of a behaviour consisting only of communication steps - taking forks, and putting them back. Even if we extend the protocol by a semaphore (inserting actions w and s before P'_i and P_i) and assume a priority of f_j^i over $b_{j\pm1}^i$ in P''_i and P'''_i (for the description of priority mechanism see [BBK2]) then the behaviour of the merge will still be unsatisfactory. Consider for instance a state Q_1 satisfying the following conditions:

$$Q(P_0) = P_0^{iv}, Q(P_1) = P'''_1, Q(P_2) = P_2, Q(P_3) = P_3^{iv}, Q(P_4) = P_4$$

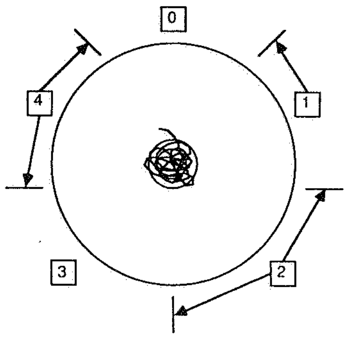
The state Q_1 may be described by the following picture:



(Here, squares are philosophers, bars denote forks, and the arrows show which forks are taken and by whom.) After executing the sequence of actions:

$$B_2^1 E_0 B_0^0 B_1^0 E_3 B_3^3 B_4^3 T_2 F_2^2 F_3^2 T_4 F_4^4 F_0^4 F_1^1$$

we get to a state Q_2 described by the picture:



Clearly, another sequence of actions will bring the system back to Q_1, and thus we obtain an infinite periodic behaviour in which P_0 performs only communicating actions. (We did not talk about semaphore in this example, but this would be still at most 3, also the priority regulation is followed.)

4.4. It is the back of what could be called fairness, what makes the protocol able to enter such a behaviour. However this is not visible from the τ_I-abstraction of the encapsulated merge. The liveness result is mainly due to the Cluster Fair Abstraction Rule, which removes from the merge all the sequences of actions providing no proper behaviour of a given component. This is necessary to avoid a behaviour in which a philosopher does not eat because he does not perform *any* action, even if he is allowed to do so. However, the rule does not distinguish between the latter situation, and that described in 4.3, and abstracts from both. This brings conclusion that our liveness property is not a sufficient basis to claim the correctness of a protocol.

4.5. We would like to formulate a condition that would imply a stronger assertion about protocols, namely fairness, understood so that all infinite behaviours of the merge contain infinitely many proper actions of a given component. Turn back to the formalism of Section 2, and take $I' = \alpha(Y)$. For $i \leqslant M, j \leqslant N$ let $\epsilon_{ij} = \partial_{\alpha(X)} \circ \tau_{I'} \circ \partial_H(X_i \| Y_j)$. We will say that the encapsulated merge $\partial_H(X_1 \| Y_1)$ is *fair* w.r.t. X iff, for all $i \leqslant M, j \leqslant N$, such that $\partial_H(X_i \| Y_j)$ is accessible, there exists a closed term t_{ij} of ACP$_\tau$, such that

$$\epsilon_{ij} = t_{ij} \cdot \delta$$

can be proved without CFAR.

4.6. Lemma. *Assume the notations from 4.5. Then the following conditions are equivalent:*

i) $\partial_H(X_1 \| Y_1)$ is fair w.r.t X;

ii) for every accessible $\tau_{I'} \circ \partial_H(X_i \| Y_j)$, $\epsilon_{ij} = \pi_{M \cdot N+1}(\epsilon_{ij}) \cdot \delta$, where π_n denotes the n^{th} projection function (see [BK4]);

iii) For every infinite path Π in $\tau_{I'} \circ \partial_H(X_1 \| Y_1)$, there is an infinite number of proper actions of X occurring along Π;

iv) For every path Π in $\partial_H(X_1 \| Y_1)$ with an infinite number of actions of X along Π, there is an infinite number of proper actions of X along Π.

Proof: (ii)⟹(i) is obvious. For (i)⟹(iii), suppose that there is a path Π in $\tau_{I'} \circ \partial_H(X \| Y)$ such that only a finite number of proper actions of X occurs along Π. Let $\tau_{I'} \circ \partial_H(X_i \| Y_j)$ be a state on Π after the last proper action of X. Since there is no more such actions on the part of Π accessible from $\partial_H(X_i \| Y_j)$, the $\alpha(X)$-encapsulated process $\epsilon_{ij} = \partial_{\alpha(X)} \circ \tau_{I'} \circ \partial_H(X_i \| Y_j)$ will still contain an infinite path, which is impossible for $\epsilon_{ij} = t_{ij} \cdot \delta$.
To prove (iii)⟹(ii) suppose that, for some i,j with $\tau_{I'} \circ \partial_H(X_i \| Y_j)$ being accessible, there is a path Π in $\tau_{I'} \circ \partial_H(X_i \| Y_j)$ such that no proper action of X occurs among the first $N \cdot M + 1$ steps of Π. Since there is at most $N \cdot M$ states of $\tau_{I'} \circ \partial_H(X_i \| Y_j)$, one of them has to be repeated, and thus there is a path Π' in $\tau_{I'} \circ \partial_H(X_i \| Y_j)$ such that no proper X-action occurs in Π'. Composing Π' with the first $NM + 1$ steps of Π we get a contradiction. Thus, an X-action has to occur among the first $NM + 1$ steps of every path in $\tau_{I'} \circ \partial_H(X_i \| Y_j)$. After the encapsulation, all paths in ϵ_{ij} are of lengths at most $MN + 1$, and all end with δ. Thus, $\epsilon_{ij} = \pi_{MN+1}(\epsilon_{ij})$, and also $\epsilon_{ij} = \epsilon_{ij} \cdot \delta$, which proves (ii).
Now, for (iii)⟺(iv) we observe that a path in $\partial_H(X_1 \| Y_1)$ with an infinite number of occurrences of X-action remains infinite in $\tau_{I'} \circ \partial_H(X_1 \| Y_1)$. On the other hand, if there were only a finite number of actions of X along Π, the path Π would be replaced in $\tau_{I'} \circ \partial_H(X_1 \| Y_1)$ by a finite subtree, because of CFAR. Hence, infinite paths in $\tau_{I'} \circ \partial_H(X_1 \| Y_1)$ correspond to paths in $\partial_H(X_1 \| Y_1)$ with X-actions occurring infinitely many times.

4.7. The above lemma explains our fairness condition. Behaviours using no proper actions of X due to the outside world are abstracted by $\tau_{I'}$, while those due to inefficient activity of X are visible in ϵ_{ij}'s. Clearly, the protocol described in 4.1 does not satisfy this condition, because of the example in 4.3. The protocol discussed in Section 3 is better.

4.8. Lemma. *Let X, Y be as in Section 3. Then $\partial_H(X \| Y)$ is fair w.r.t X.*

Proof: It is not difficult to see that $\tau_{I'} \circ \partial_H(X_i \| Y_j) + \tau_{I'} \circ \partial_H(X_i) = \tau_{I'} \circ \partial_H(X_i)$ for all accessible $\partial_H(X_i \| Y_j)$ since both the components are sums, all the summands of the first occurring in the second one. Further, for regular processes it holds that $x + y = z\delta$ implies $x = v\delta$, for some v. (To see this, consider a bisimulation R between $x + y$ and $z\delta$. The image of the nodes of x defined by R is a subtree of $z\delta$, representing the regular process $v\delta$). Thus, it is enough to prove for all i that $\partial_{\alpha(x)} \circ \tau_{I'} \circ \partial_{H'}(X_i) = t_i\delta$, for some closed t_i, which is obvious.

4.9 Remark: If we allow philosophers to take an arbitrary fork first (but not to put it back before eating), and we use a semaphore, we get a non-linear protocol satisfying also the fairness condition. The proof is exactly the same as that of lemma 4.8.

4.10. It should be a matter of further research to develop a method of proving the fairness condition in a more purely algebraic way, or to reformulate it in a more convenient form - it is unsatisfactory that our condition is formulated using the notion of a closed term and existential quantification, or the size of the processes under consideration.

4.11. However, even if we are concerned with the liveness condition only, the situation is not hopeless. From some point of view, protocols satisfying this condition *are* fair. Assume that the choices between actions in the merge are made by a schedular, according to some probability distributions defined for all accessible $\partial_H(X_i \| Y_j)$ and assigning non-zero probabilities to all the possible actions. We will say that $\partial_H(X \| Y)$ is probabilistically fair w.r.t. X iff the probability of obtaining a path in $\partial_H(X \| Y)$ involving only a finite number of proper actions of X is zero. A similar observation to the following one may be also found in [P].

4.12. PROPOSITION. *If X is uniformly live in $\partial_H(X \| Y)$ then $\partial_H(X \| Y)$ is probabilistically fair w.r.t. X, provided $\alpha(X_i) - H \neq \emptyset$, for all $i \leq M$.*

PROOF: Let $\partial_H(X_i \| Y_j)$ be accessible. There exists n_i such that a state $X_{i'}$ allowing an action proper for X is accessible from X_i in n_i steps. Clearly, because of the finiteness of the processes, there exists a common upperbound n for all these n_i's. It is not difficult to see then that there is a non-zero probability of performing in n steps at least one action proper for X, from any given accessible state. Thus, the probability of not performing such an action at all is a limit of a decreasing geometrical progress and thus has to be equal to 0. The probability of a finite number of proper actions of X is also 0, as an enumerable sum of 0's.

ACKNOWLEDGEMENTS

This work was prepared during my stay at the Centrum voor Wiskunde en Informatica. I wish to thank the colleagues from CWI, especially Jos Baeten, Jan Bergstra and Frits Vaandrager, for their inspiration, helpful comments and many discussions.

REFERENCES

[B-A] BEN-ARI, M., *Principles of concurrent programming,* Prentice-Hall, 1982.

[BBK1] BAETEN, J.C.M., J.A. BERGSTRA & J.W. KLOP, *Conditional axioms and α / β calculus in process algebra,* CWI Report CS-R8502, Amsterdam 1985.

[BBK2] BAETEN, J.C.M., J.A. BERGSTRA & J.W. KLOP, *Syntax and defining equations for an interrupt mechanism in process algebra,* CWI Report CS-R8503, Amsterdam 1985.

[BK1] BERGSTRA, J.A. & J.W. KLOP, *Algebra of communicating processes with abstraction,* Theor. Comp. Sci. 37(1), pp. 77-121, 1985.

[BK2] BERGSTRA, J.A. & J.W. KLOP *Verification of an alternating bit protocol by means of process algebra,* CWI Report CS-R8404, Amsterdam 1984.

[BK3] BERGSTRA, J.A. & J.W. KLOP, *A complete inference system for regular processes with silent moves,* CWI Report CS-R8420, Amsterdam 1984.

[BK4] BERGSTRA, J.A. & J.W. KLOP, *Algebra of communicating processes,* CWI Report CS-R8421, Amsterdam, 1984.

[BKO] BERGSTRA, J.A., J.W. KLOP & E.-R. OLDEROG, *Failure semantics with fair abstraction,* CWI Report CS-R8609, Amsterdam 1986.

[P] PNUELI, A., *On the extremely fair treatment of probablistic algorithms,* Proc. 15th STOC, Boston, 1983.

[V] VAANDRAGER, F.W., *Verification of two communication protocols by means of process algebra,* CWI Report CS-R8608, Amsterdam, 1986.