A Process Algebra for Timed Systems*

Matthew Hennessy, Tim Regan
University of Sussex

Abstract: A standard process algebra is extended by a new action σ which is meant to denote *idling* until the next clock cycle. A semantic theory based on testing is developed for the new language. This is characterised in terms of *barbs*, a variety of ready traces and also characterised as the initial theory generated by a set of equations.

1 Introduction

Process algebras are structured high-level description languages for concurrent systems, [Mil89, Hoa85, BW90a]. They consist of a small number of constructors or combinators for building processes together with a facility for recursive definitions. They have a range of well-developed semantic theories and related proof systems associated with them and they have been shown to be reasonably successful for both the specification and verification of concurrent systems, [BW90b]. Intuitively they view processes as objects which are capable of performing "abstract actions" which are usually interpreted as the input or output of values or signals along communication channels. These capabilities are expressed in terms of "next-state relations", $\longrightarrow$, between processes; $p \xrightarrow{a} q$ represents the fact that the process p can perform the action a and thereby evolve into the process q. This is a relatively abstract interpretation of process. For instance there is no mention of the length of time the action a takes, or when the action occurs or indeed that it actually occurs at all; $p \xrightarrow{a} q$ merely says that the process p has the capability of performing the action a. However this abstract view turns out to be a major contributing factor to the success of process algebras; it enables one to describe systems at different levels of abstraction and to relate these different descriptions via semantic equivalences. For example one high-level description S could be viewed as a desired specification of a system and a lower-level description I a description of an actual implementation and proving S semantically equivalent to I amounts to showing that the implementation satisfies the required specification.

Time is often an important aspect of the description of many concurrent systems but it is not directly represented in any of the standard process algebras such as *CCS, CSP* and *ACP*. The introduction of aspects of time into the setting of process algebras has received much attention in recent research and not surprisingly, considering the fact that time is a complex subject, there have been many proposals, [BB89, DS89, NRSV92, MT90a, Re88, Yi90]. This paper presents another proposal. Our viewpoint may best be explained by contrast with the approaches of say [BB89, Re88]. These papers suggest

*The authors would like to acknowledge the financial support of British Telecom RT6224, the ESPRIT II-BRA project CONCUR and the SERC.

very descriptive languages with which one may describe the minutiae of detailed timing considerations in complex systems. Such languages are certainly required but there are certain applications, those in which time plays a restricted role, for which these languages may be inappropriate because the descriptions may be unnecessarily complex. Our proposal is quite modest: we wish to make a relatively minor extension to a standard process algebra with a mathematically simple notion of time which, although not universally applicable, will be sufficiently useful in particular application areas such as protocol verification. Protocols are a typical example of systems where timing considerations affect the behaviour of only a small part of the overall system. Our language is designed so that specification of the time-independent part of the system may be carried out as usual while the time-dependent part may be treated with our time-based extension. We hope that by introducing a simple notion of time many of the characteristics of standard process algebras which have made them so successful will still be retained in the enlarged setting. In particular we wish to extend the semantic theory of processes based on testing, [He88], to a setting where time plays a significant role. From a methodological point of view it seems appropriate to start with a language in which the concept of time is rather simple.

The idea is to introduce into a standard process algebra, *CCS*, a σ action. The execution of this σ action by a process indicates that it is idling or doing nothing until the next clock cycle. This action will share many of the properties of the standard actions of *CCS* but because it represents the passage of time it will be distinguished from the standard actions by certain of its properties. For example in our process algebra this action will be *deterministic* in the sense that a process can only reach at most one new state by performing σ . This is a reflection of the assumption that the passage of time is deterministic. There is also an intuitive assumption underlying the usual (asynchronous) theories of process algebras, such as *CCS* as expounded in [Mil89] and *CSP* as expounded in [Hoa85], that all processes may idle indefinitely and the semantic theory is formulated in terms of the actions which a process may perform, if it so wishes. Indeed, this view of processes is investigated in detail in [Mil83]. We continue to use this assumption; using the syntax of *CCS,* the process $a.p$ can idle, i.e. it can perform a σ action. This means that we assume all processes are *patient* in that they will wait indefinitely until communications in which they can participate become possible. Moreover this means that the implicit assumption underlying *CCS* that all communication actions are instantaneous is retained in our language since we have a distinguished action σ denoting the passage of time and, as we will see, all other actions are performed in between occurrences of this time action. However, we add one further assumption, namely that communications must occur if they are possible: a process cannot delay if it can perform a communication. This we call the *maximal progress* assumption, [HdR89], which is a common feature of many proposed timed process algebras. So, again using the syntax of *CCS*, although $a.p + b.q$ can idle, $(a.p + b.q)|\overline{a}.q$ cannot idle; the communication via the a channel must occur. However we are not simply giving a mild re-interpretation to *CCS*. Because of the presence of σ in the language we can express processes whose behaviour is, at least to some extent, time-dependent. The new action does not only indicate idleness but also forced delay; $\sigma.a.p$ is a process which can do nothing until the first clock cycle and from that moment on it offers an a action.

Thus our approach to the introduction of time into process algebras may be characterised by five intuitive properties:

1. *discrete time:* in our language time proceeds in discrete steps represented by occurrences of the action σ,

2. *time determinism:* we assume that the passage of time is deterministic,

3. *actions are instantaneous:* time is not associated directly with communication actions but occurs independently,

4. *patience:* processes will wait indefinitely until they can communicate

5. *maximal progress:* processes communicate as soon as a possibility for communication arises.

Of course none of these assumptions are necessary in a timed process algebra and in our comparison with related work we will discuss languages in which combinations of these assumptions are dropped. However we hope to convince the reader that their adoption leads to a calculus which

1. on the one hand is mathematically tractable ; we demonstrate this by extending the theory of testing from [dNH84, He88] to this timed setting. This theory may be characterised equationally in a manner which differs only slightly from a standard theory of *CCS*, [dNH84]; moreover there is a close connection with the theory of refusals, [Ph87].

2. on the other may be successfully applied to certain application areas; We demonstrate this by treating a relatively simple example of a protocol in which time plays a small but significant role. Further more substantial examples may be found in [Rea91].

As stated previously we do not expect our calculus to be applicable to all manner of timed systems. But we believe it is applicable; moreover it offers the advantage of relative simplicity with a fully developed semantic theory and therefore we hope that it provides a sound basis on which to develop more extensive theories of timed systems.

We end this introduction with an outline of the contents of the the remainder of the paper. In the next section we give the syntax of our timed process algebra *TPL*, which stands for *Timed Process Language*, together with an operational semantics. Using this operational semantics we then define an operational preorder on timed processes based on the *must* testing from [dNH84, He88]. This is a standard application of the testing scenario from [He88] but here the tests may use the timing constructs from *TPL* and therefore the power of testing is considerably increased. In the next section, Section 3, we give an alternative characterisation of the testing preorder. For the untimed language this alternative characterisation is given in terms of *acceptances*, [He88] which are of the form sA; here s is a sequence of actions a process can perform to a state in which one of the actions from the finite set A can be performed. Because timed tests are more powerful the alternative characterisation for *TPL* has to take into account more of the behaviour of processes. It is expressed in terms of *barbs*, [Pn85, vG88], which are sequences of the form $s_1A_1s_2\ldots s_kA_k$. Section 4 is devoted to an equational characterisation of the behavioural preorder. This is in terms of a proof system which consists of a set of equations, a slight weakening of the equational theory of *CCS* from [dNH84] together with an infinitary rule for recursively defined processes, again as used in [dNH84, He88] and a new rule for *patient* processes. In the next section we develop a prototypical example of where we believe our simple assumptions about time can be of use. It is a straightforward protocol for transferring messages across a faulty medium. More extensive examples can be found in [Rea91]. In the final section we describe some related work on timed process algebras. The literature in this area of research is quite extensive and so we confine our discussion to approaches which are quite similar to ours.

2 Syntax and Behavioural Semantics

In this section we present the process algebra *TPL* (Temporal Process Language) formally and develop a behavioral theory of these processes based on "must" testing, [He88]. We define the language as closed terms built from a set of constructors, give an operational semantics for the language in terms of *labelled transition systems* and finally define a behavioural preorder based on testing.

The abstract syntax of the language is given by the following BNF definition:

$$t ::= nil \mid \Omega \mid x \mid \sigma.t \mid \lfloor t \rfloor (t) \mid a.t \mid \tau.t \mid t + t \mid t|t \mid t[S] \mid t \setminus a \mid recx.t$$

where a ranges over Act, a set of actions not containing the distinguished actions τ and σ . The operator $recx.\_$ acts in the usual way as a binder for variables and we are mainly interested in closed terms which we call processes. We will use meta-variables p, q etc. to range over these processes, a, b, c to range over the set of actions Act and Greek letters α, β (but not ω or σ) to range over Act_τ, the union of Act and $\{\tau\}$. We will not often need to talk about a general action from $Act \cup \{\tau\} \cup \{\sigma\}$ and so this will be explicitly stated where necessary.

We give some intuition of these operators, discussing each in turn.

- *nil*. This is the process which is terminated or deadlocked; it can perform no actions from Act_τ but as discussed in the introduction we design our language so that all processes are *patient* and for this reason *nil* will allow the passage of time, i.e. it can idle indefinitely.

- Ω. This process represents incomplete information or divergence. This incomplete knowledge of a process is catastrophic in that a process whose behaviour is not completely determined will be equivalent to one whose behaviour is completely unknown.

- $a.$. The process $a.p$ can perform an action a and in so doing evolve into the process p. As is usual in *CCS* style languages there is an overbar or complementary function $Act \rightarrow Act$ which is idempotent and is used to formalise synchronisation. Again because we wish all our processes to be *patient* $a.p$ will be able to idle indefinitely until until the a action is requested by that environment.

- $\tau.$. This is the silent or internal action of our language. Since we are imposing the assumption of maximal progress the process $\tau.p$ will not be able to idle in any environment. The τ action represents some internal communication or computation which requires nothing of the environment. When it is possible τ will preempt any passage of time. An intuition for this is that if a process is offering an action a which is requested by another process by the offer of an action $\overline{a}$, we do not want unspecified delay to occur; the communication, the τ move, must fire immediately.

- σ.. The passage of time is modelled in our system by an occurance of a σ action. As discussed in the introduction this represents a relatively abstract notion of time but it can be intuitively thought of as the click of a clock which measures the passage of time for the system. We chose σ as the symbol to represent the passage of time because of its similarity to Phillips 'broadcast stability operator' of [Ph87].

- $+$. Deterministic and nondeterministic choice between two processes is modelled in *CCS* by the operator $+$. For actions a in *Act* and the action τ the operator $+$ behaves in the same way as it does in the *CCS* setting. The difference comes with the action σ . If two processes are just idling before the environment requests one of them the choice between them will not be made by the passage of time alone. That is to say that $+$ is not decided by the action σ . This is necessary to ensure that the passage of time is deterministic.

- $\lfloor\ \rfloor(\ )$. This operator comes from the process algebra *ATP* put forward in [NRSV92]. It is similar to the context $\_ + \sigma.\tau.\_$ but is properly decided by the passage of time in favour of the right hand operand. This operator will be used in the complete axiomatisation of the full calculus although it is also useful in many examples.

- $|$. The parallel bar we use is the handshake and interleaving of *CCS*. However σ again behaves differently. When two processes traverse time their composition also does. This is represented by σ being a broadcast event over $|$ and again this is necessary if we wish to ensure that time is deterministic.

- $\backslash a$. This is just the restriction operator of *CCS*. It is quantified over *Act* but we often use the shorthand $\backslash A$ to mean $\backslash a_1 \backslash a_2 \backslash a_3 ... \backslash a_n$ where $A = \{a_1, a_2, a_3, ..., a_n\}$. Although it has the same syntax as the *CSP* and *LOTOS* hiding operators it has a very different operational meaning. For us the context $\_ \backslash a$ forbids the action a and $\overline{a}$.

- $[S]$. This is the relabelling operator from *CCS*. Here S is function from *Act* to *Act* which is almost everywhere the identity and which preserves the complement function. In practice we assume that such functions are automatically extended so that $S(\tau) = \tau$ and $S(\sigma) = \sigma$. Relabeling functions enable the re-use of processes in situations demanding the same functionality modulo action names.

From this informal description of the language we see that *CCS* is a sub-language of *TPL* and therefore we say that a process from *TPL* is a *CCS* process if it does not use the timing constructs σ and $\lfloor\ \rfloor(\ )$.

The operational semantics of processes is given in two parts. The first, in Figure 1, defines the next state relations, $\xrightarrow{\alpha}$, for each $\alpha \in Act_\tau$. This is a slight generalisation of the standard operational semantics for *CCS* and the new action σ plays no role. In Figure 2 the relation $\xrightarrow{\sigma}$ is then defined in terms of these relations. The first rule says that both $a.p$ and nil may delay. This is a perfectly reasonable assumption; if $a.p$ is in an environment where no communication via a is possible, then it should be allowed

$$ACT_1 : \frac{}{\alpha.p \xrightarrow{\alpha} p}$$

$$SUM_1 : \frac{p \xrightarrow{\alpha} p'}{p + q \xrightarrow{\alpha} p'} \qquad SUM_2 : \frac{q \xrightarrow{\alpha} q'}{p + q \xrightarrow{\alpha} q'}$$

$$THEN_1 : \frac{p \xrightarrow{\alpha} p'}{\lfloor p \rfloor (q) \xrightarrow{\alpha} p'}$$

$$COM_1 : \frac{p \xrightarrow{\alpha} p'}{p|q \xrightarrow{\alpha} p'|q} \qquad COM_2 : \frac{q \xrightarrow{\alpha} q'}{p|q \xrightarrow{\alpha} p|q'}$$

$$COM_3 : \frac{p \xrightarrow{a} p',\ q \xrightarrow{\overline{a}} q'}{p|q \xrightarrow{\tau} p'|q'}$$

$$REL_1 : \frac{p \xrightarrow{\alpha} p'}{p[S] \xrightarrow{S(\alpha)} p'[S]} \quad RES_1 : \frac{p \xrightarrow{\alpha} p',\ \alpha \notin \{b, \overline{b}\}}{p \setminus b \xrightarrow{\alpha} p' \setminus b}$$

$$REC_1 : \frac{t[recx.t/x] \xrightarrow{\alpha} p'}{recx.t \xrightarrow{\alpha} p'}$$

Figure 1: Standard Operational Semantics

to delay until the next time cycle. Similarly, *nil* may delay indefinitely as it can never perform a communication. Note, however, that $\tau.p$ cannot delay; it must perform the internal move τ before the next time cycle. The third rule says that $p + q$ may delay if both p and q may delay. Note that the passage of time, i.e. performing a σ action, does not decide between the choice in $p + q$. The fourth rule says that $p|q$ may delay if both p and q may delay and no communication between p and q is possible. The other rules are straightforward; the final rule represents the standard methods for handling restriction and recursion while the rule for $\sigma.p$ is perfectly natural.

We now give some examples of processes which may help to explain the influence of σ on the power of the language. In these examples we use the informal notation of recursive definitions rather than $recx.\_$. We will also use the standard conventions in writing *CCS* terms: occurrences of *nil* will often be omitted, action prefixing will have higher precedence than restriction and relabelling, both of which will in turn be higher than | which will bind tighter than +.

Example 2.1 A process that may accept a message and transmit it back to the environment, retransmiting every one time unit until an acknowledgement is received could be written:

$$\begin{array}{rcl} P & \Longleftarrow & message_{in}.\overline{message}_{out}.P' \\ P' & \Longleftarrow & ack.P + \sigma.\overline{message}_{out}.P'. \end{array}$$

$$ACT_2 : \frac{}{a.p \xrightarrow{\sigma} a.p} \qquad NIL : \frac{}{nil \xrightarrow{\sigma} nil}$$

$$WAIT : \frac{}{\sigma.p \xrightarrow{\sigma} p}$$

$$SUM_3 : \frac{p \xrightarrow{\sigma} p',\ q \xrightarrow{\sigma} q'}{p + q \xrightarrow{\sigma} p' + q'}$$

$$THEN_2 : \frac{p \not\xrightarrow{\tau}}{\lfloor p \rfloor (q) \xrightarrow{\sigma} q}$$

$$COM_4 : \frac{p \xrightarrow{\sigma} p',\ q \xrightarrow{\sigma} q',\ p|q \not\xrightarrow{\tau}}{p|q \xrightarrow{\sigma} p'|q'}$$

$$REL_2 : \frac{p \xrightarrow{\sigma} p'}{p[S] \xrightarrow{\sigma} p'[S]} \quad RES_2 : \frac{p \xrightarrow{\sigma} p'}{p \setminus a \xrightarrow{\sigma} p' \setminus a}$$

$$REC_2 : \frac{t[recx.t/x] \xrightarrow{\sigma} p'}{recx.t \xrightarrow{\sigma} p'}$$

Figure 2: Operational Semantics for σ

□

Example 2.2 The process Egg_1 is defined so that if left too long before eating the egg MAY be unhealthy (and may not).

$$Egg_1 \Leftarrow \overline{eat}.healthy.nil + \sigma.\sigma.\overline{eat}.unhealthy.nil.$$

The process Egg_2 is defined so that if left too long before eating the egg WILL be unhealthy.

$$Egg_2 \Leftarrow \lfloor \overline{eat}.healthy.nil \rfloor (\lfloor \overline{eat}.healthy.nil \rfloor (\overline{eat}.unhealthy.nil))$$

□

Example 2.3 A "leaking counter" defined informally as

$$\begin{aligned} C_0 &\Longleftarrow press.up.C_1 \\ C_{n+1} &\Longleftarrow press.up.C_{n+2} + \sigma.down.C_n. \end{aligned}$$

It can perform on *up* action each time it is *pressed* but if no *press* is forthcoming before the next clock cycle it can perform a *down* action. So, for example, $(C_0|\overline{press}^k) \setminus press$ acts like the process $up^k.(\sigma.down)^k$. □

Some of the informal assumptions underlying the design of the language which we discussed in the introduction can now be seen to be reflected in the operational semantics. This is the import of the following proposition:

Proposition 2.4

1. *(Time-determinism) if $p \xrightarrow{\sigma} q$ and $p \xrightarrow{\sigma} q'$ then q and q' are syntactically the same*

2. *(Maximal progress) if $p \xrightarrow{\tau} q$ then $p \xrightarrow{\sigma} r$ for no process r*

Proof: By induction on the length of the proof of $p \xrightarrow{\sigma} q$, $p \xrightarrow{\tau} q$ respectively. □

The informal assumption of *patience* is not as straightforward to capture. Intuitively this should state that if a process p can not perform a τ action then it must be able to delay, i.e. perform a σ action. But because of the presence of recursive definitions the situation is more complicated. For example the processes $recx.x$ and Ω can perform no action whatsoever. Intuitively these terms represent under-defined or "badly defined processes" and therefore they require special attention. Terms which intuitively represent well-defined processes are captured in the following definition:

Definition 2.5 (Strong Convergence)
Let $\downarrow$ be the least (postfix) predicate over *TPL* which satisfies

$$\begin{array}{rl} i) & nil \downarrow,\ \alpha.p \downarrow,\ \sigma.p \downarrow \\ ii) & p \downarrow \text{ implies } (\lfloor p \rfloor (q)) \downarrow, (p|q) \downarrow,\ p \setminus a \downarrow,\ p[S] \downarrow, \\ iii) & p \downarrow,\ q \downarrow, \text{ implies } (p+q) \downarrow, \\ iv) & t[recx.t/x] \downarrow \text{ implies } recx.t \downarrow . \end{array}$$

□

We write $p \uparrow$ to denote the negation of $\downarrow$ and one can check that, for example, $\Omega \uparrow$ and $recx.x \uparrow$. With this new notation we can now see how *patience* is reflected in our operational semantics.

Proposition 2.6 *(Patience) If $p \downarrow$ and $p \xrightarrow{\tau} q$ for no process q then there exists a process r such that $p \xrightarrow{\sigma} r$*

Proof: By induction on the proof that $p \downarrow$. □

We now turn our attention to the definition of a behavioural preorder between processes. We follow the approach of [He88] which is based on testing and for convenience we only consider the "must" case. However, because *TPL* is an extension of *CCS*, the definitions we employ will be based on those from [dNH84] where the predicate $\downarrow$ plays a necessary role. A test e is a process from *TPL* which may additionally use the special action ω for reporting success. A test e is applied to a process p by "running" the process

$e|p$, i.e. allowing it to evolve via τ actions or σ actions. Specifically a *computation* from $e|p$ is a maximal sequence (which may be finite or infinite) of the form

$$e|p = e_0|p_0 \mapsto e_1|p_1 \mapsto \ldots \mapsto e_i|p_i \mapsto \ldots \quad (\text{where} \mapsto = \xrightarrow{\tau} \cup \xrightarrow{\sigma})$$

To say when such an application is a success we need the notion of strong convergence defined above.

We say p *must* e if in every computation from $e|p$,

$$e|p = e_0|p_0 \mapsto \ldots \mapsto e_k|p_k \mapsto \ldots$$

there exists some $n \geq 0$ that $e_n \xrightarrow{\omega}$, i.e. e_n can report success, and for every $k, 0 \leq k < n \;\; e_k|p_k \downarrow$. Finally, we say that

$$p \mathrel{\underset{\sim}{\sqsubset}} q$$

if for every test e, p *must* e implies q *must* e. We use $\eqsim$ to denote the kernel of this preorder.

The definition of $\mathrel{\underset{\sim}{\sqsubset}}$ is close to that employed in [dNH84] and, therefore, if we restrict both the processes and the tests to *CCS* the resulting theory is exactly that developed in [dNH84]. However here we also allow occurrences of σ in the tests and these new tests, even when applied to *CCS* terms, i.e. terms not involving the timing constructs σ and $\lfloor\;\rfloor(\;)$, have more distinguishing power than standard *CCS* tests. An interesting difference in the power σ vests in testing languages can be found in [La89]:

Example 2.7 This example concerns two vending machines (shown diagrammatically in Figure 3 where σ actions are ignored) with slightly different internal behaviour

$$coin.(tea + hit.tea) + coin.(coffee + hit.coffee)$$

and

$$coin.(tea + hit.coffee) + coin.(coffee + hit.tea).$$

These are equivalent in the standard theory but they can be distinguished by the temporal test $\overline{coin}.(\overline{tea}.\omega + \sigma.\overline{hit}.\overline{tea}.\omega)$, a test which says that if you can not do a *tea* action immediately after doing a *coin* action then you will be able to do so after performing a *hit* action. $\square$

This kind of testing of *CCS* processes has already been introduced in [Ph87] and [Ph88] and for *LOTOS* in [La89]. Indeed, as mentioned, we have borrowed the notation used by Phillips for his stability operator in [Ph88] for our new delay action, although there is a significant difference: his delay operator decides $+$ whereas ours does not. It should be emphasised that both authors introduce these operators into the test language only and not into the process language.

The preorder $\mathrel{\underset{\sim}{\sqsubset}}$ is not a congruence with respect to the operators $+$ and $\lfloor\;\rfloor(\;)$. For $+$ the example is the usual one: $a.nil \mathrel{\underset{\sim}{\sqsubset}} \tau.a.nil$ but $b.nil + a.nil \mathrel{\underset{\sim}{\sqsubset}} b.nil + \tau.a.nil$ is not true. One can also check that $\lfloor \tau.a \rfloor(b) \eqsim \tau.a$ but $\lfloor a \rfloor(b)$ is obviously not equivalent to $\tau.a$. However, as we will see, the standard approach to generating a precongruence from $\eqsim$ will also work for our language: let $p \mathrel{\underset{\sim}{\sqsubset}}^{+} q$ if for some a not occurring in p and $q \quad a.nil + p \mathrel{\underset{\sim}{\sqsubset}} a.nil + q$. In the next section we will prove that $p \mathrel{\underset{\sim}{\sqsubset}}^{+} q$ is the largest preorder contained in $\mathrel{\underset{\sim}{\sqsubset}}$ which is preserved by all the operators of the language, nil, $\mu.$, $+$, $\lfloor\;\rfloor(\;)$, $|$, $\backslash a$ and $[S]$.

So now we have a fully fledged process language endowed with a behavioral preorder. In the next section we present an alternative characterisation in terms of barbs, [Pn85].

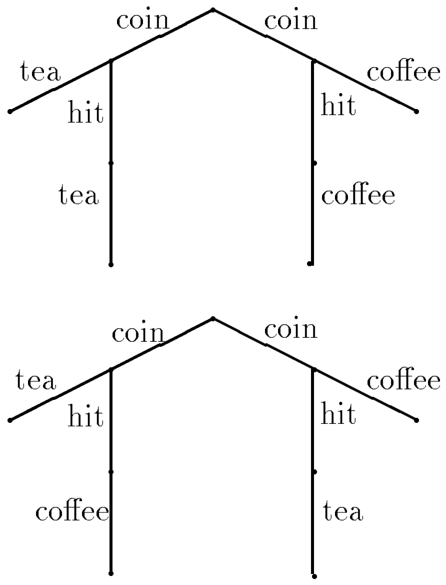


Figure 3: Langerak's Vending Machines

3 Alternative Characterisation

In this section we look at an alternative characterisation of $\underset{\sim}{\sqsubset}$ over *TPL*. The corresponding alternative characterisation for the untimed language in [He88] is in terms of "acceptances" of the form sA where s is a sequence of actions a process can perform to arrive at a state and A is the set of next possible actions which can be performed from that state. However because of the presence of the timing constructs in the tests for *TPL* the characterisation now needs to be more complicated. The necessary behavioural information can be encoded in a manner similar to the barbs of [Pn85] which are closely related to the *failure traces* of [vG88]. However because of the presence of σ in processes and the treatment of divergence care must be taken in the definition of barbs and how they are associated with processes.

Definition 3.1 (Barbs) Let the set of barbs be the least set satisfying :

1. Ω is a barb
2. if A is a finite subset of *Act* then A is a barb
3. if $\underline{b}$ is a barb and $a \in Act \cup \{\sigma\}$ then $a\underline{b}$ is a barb
4. if $\underline{b}$ is a barb and A is a finite subset of *Act* then $A\underline{b}$ is a barb

□

Thus a barb may be viewed as a sequence of the form

$$s_1A_1s_2A_2...s_kA_k$$

or

$$s_1A_1s_2A_2...s_k\Omega$$

with $1 \leq k$ where $s_i \in (Act \cup \sigma)^*$ and each A_i is a finite subset of Act. These barbs may be compared using the following order:

Definition 3.2 $\ll$ is the least preorder over barbs which satisfies

1. $\Omega \ll \underline{b}$.
2. $A \subseteq B$ implies $A \ll B$
3. $\underline{b} \ll \underline{b'}$ implies $a\underline{b} \ll a\underline{b'}$
4. $\underline{b} \ll \underline{b'}$ and $A \subseteq A'$ implies $A\underline{b} \ll A'\underline{b'}$

□

This ordering is lifted to sets of barbs by defining

$$A \ll B \ \Leftrightarrow \ \forall \underline{b} \in B . \exists \underline{a} \in A . \underline{a} \ll \underline{b}.$$

In order to associate barbs with processes we have to introduce some notation. First the relations $\xrightarrow{\mu}$ are extended to $\xrightarrow{s}$, for $s \in (Act \cup \{\sigma, \tau\})^*$, in the obvious way. Also $\overset{\lambda}{\Longrightarrow}$, $\lambda \in Act \cup \{\sigma\}$, is used to denote $\xrightarrow{\tau}^* \xrightarrow{\lambda} \xrightarrow{\tau}^*$ and this is also extended to $\overset{s}{\Longrightarrow}$, $s \in (Act \cup \{\sigma\})^*$, in the natural way. Let

$$\begin{array}{rcl} S(p) & = & \{a : p \xrightarrow{a}, a \in Act\} \\ Sort(p) & = & \{a : p \overset{s}{\Longrightarrow} p' \xrightarrow{a}, \ s \in (Act \cup \{\sigma\})^*, a \in Act\}. \end{array}$$

We next generalise the strong convergence predicate $\downarrow$ to take internal actions into account: Let $\Downarrow$ be the least predicate on TPL which satisfies

$$p \downarrow \ and \ \forall p'.(p \xrightarrow{\tau} p' \Rightarrow p' \Downarrow) \ \ implies \ \ p \Downarrow .$$

We use $p \Downarrow$ to denote the negation of $p \Uparrow$. Finally we say p is *stable* if $p \downarrow$ and $p \not\xrightarrow{\tau}$, i.e. for no p' is $p \xrightarrow{\tau} p'$. Sometimes we will just want to say p cannot perform a τ move in which case we will call p τ-stable. So for example $a.p$ is both stable and τ-stable while $a.p + \Omega$ is just τ-stable.

Now consider a barb of the form

$$s_1 A_1 s_2 A_2 ... s_k B$$

where B is either Ω or another finite subset of Act. This barb can be generated by the process p if there exists a derivation of stable processes $p_1, p_2, \ldots, p_k$:

$$p \overset{s_1}{\Longrightarrow} p_1 \overset{s_2}{\Longrightarrow} p_2 \ldots \overset{s_k}{\Longrightarrow} p_k$$

with $A_i = S(p_i)$ for $1 \leq i \leq k-1$ and if B is Ω then $p_k \Uparrow$ and otherwise p_k is also stable with $B = S(p_k)$. Let $Barbs(p)$ be the set of barbs generated by the process p.

Definition 3.3 For TPL processes p and q let $p \ll^r q$ iff $Barb(p) \ll Barb(q)$. □

The r superscript in this definition stands for *regular* since, although this ordering serves as an alternative characterisation for *CCS* (as the next theorem states), it is inadequate for *TPL*. We will need to restrict our attention to a specialisation of barbs to obtain an alternative characterisation of *TPL*. The reason for this is that any stable *CCS* process may perform a σ action to itself whereas this is not true in *TPL* (e.g. $\lfloor a.nil \rfloor (b.nil)$). It is also worth pointing out that this definition differs from that in [HR90]. There the definition of $\ll^r$ is defined in terms of the preorder $<$ and convergence of processes over barbs, a concept we have not defined. We prefer here to define $\ll^r$ in terms of the sets of barbs alone. This substantially reduces the amount of work involved in checking the equivalence of processes in next section's soundness proof.

Theorem 3.4 *(Alternative Characterisation for CCS) For p,q in CCS, $p \underset{\sim}{\sqsubset} q$ if and only if $p \ll^r q$.* □

It is worth pointing out that this theorem is not true if we restrict *Barb(p)* to simple barbs, i.e. those where each sequence s_i is of length at most one. For example, let p denote the process $d.(a.nil + c.nil | \overline{c}.nil) \setminus c$. Then both p and $d.nil$ have exactly the same simple barbs, namely prefixes of $\varepsilon\{d\}d\emptyset$. However they can be distinguished by the test $\overline{d}.(\overline{a}.nil + \sigma\omega)$.

The theorem is also not true for the entire language *TPL* as barbs are too discriminating. For example

$$\tau.(b.nil + \sigma.a.nil) + \tau.(a.nil + c.nil) \not\ll^r a.nil + b.nil$$

because the barb $\{a, b\}a$ distinguishes them although (as we will soon be able to verify) they are related via $\underset{\sim}{\sqsubset}$.

To characterise $\underset{\sim}{\sqsubset}$ over *TPL* we need to restrict ourselves to *standard* barbs, i.e. barbs of the form

$$s_1 A_1 \sigma s_2 A_2 \sigma s_3 ... s_k A_k$$

or

$$s_1 A_1 \sigma s_2 A_2 \sigma s_3 ... s_k \Omega$$

where each s_i is now a member of the set Act^* i.e. they do not contain occurances of σ .

Let $SBarb(p)$ be the standard barbs associated with the process p and (by overloading notation) $\ll$ the modification to $\ll^r$ which restricts attention to standard barbs. We may now state the main result of this section:

Theorem 3.5 *(Alternative Characterisation for TPL) For p,q in TPL, $p \underset{\sim}{\sqsubset} q$ if and only if $p \ll q$.*

The remainder of this section is devoted to proving this characterisation of $\underset{\sim}{\sqsubset}$ over *TPL*. The proof of the corresponding characterisation for *CCS*, Theorem 3.4, is omitted as it is very similar.

Proposition 3.6 *For p,q in TPL $p \ll q$ implies $p \underset{\sim}{\sqsubset} q$.*

Proof: Let us assume $p \ll q$ and p *must* e. We prove q *must* e by examining an arbitrary computation from $e|q$:

$$C \equiv e|q = e_0|q_0 \mapsto e_1|q_1 \mapsto \ldots e_i|q_i \mapsto \ldots \tag{1}$$

Each move $\mapsto$ may either be $\xrightarrow{\sigma}$ or $\xrightarrow{\tau}$ and let us concentrate on the former. Then (1) may be rewritten in the form

$$C \equiv e|q = e_0|q_0 \xrightarrow{\tau}{}^{*} f_1|r_1 \xrightarrow{\sigma} \xrightarrow{\tau}{}^{*} f_2|r_2 \ldots e_i|q_i \xrightarrow{\sigma} \xrightarrow{\tau}{}^{*} \ldots \tag{2}$$

where each $f_i|r_i$ corresponds to some $e_j|q_j$, $j \geq 1$. Note that this sequence of $f_i|r_i$'s may be finite even if the origional sequence is infinite. Now this computation may be "unzipped" to reveal the contributions from the test and process:

$$\begin{aligned} &q_0 \overset{s_1}{\Longrightarrow} r_1 \xrightarrow{\sigma} \overset{s_2}{\Longrightarrow} r_2 \xrightarrow{\sigma} \ldots \\ &e_0 \overset{\overline{s_1}}{\Longrightarrow} f_1 \xrightarrow{\sigma} \overset{\overline{s_2}}{\Longrightarrow} f_2 \xrightarrow{\sigma} \ldots \end{aligned} \tag{3}$$

For the moment let us assume that each e_i in the computation is strongly convergent. This allows us to concentrate on the derivation from q_0. It gives rise to the sequence of barbs from $SBarb(q)$:

$$\begin{array}{ll} \underline{b_1}: & s_1S(r_1) \\ \underline{b_2}: & s_1S(r_1)\sigma s_2S(r_2) \\ . & \\ . & \\ . & \\ \underline{b_k}: & s_1S(r_1)\sigma s_2S(r_2)\sigma s_3 ... s_kS(r_k) \\ . & \\ . & \\ . & \end{array}$$

This sequence may terminate with a barb $\underline{b_m} = s_1S(r_1)\sigma s_2S(r_2)\sigma s_3 ... s_m\Omega$ or it may well be infinite. Note that it cannot terminate with a barb $\underline{b_m} = s_1S(r_1)\sigma s_2S(r_2)\sigma s_3 ... s_mS(r_m)$ since this would imply that both the experiment and the q are in a stable position with no communication possible and that q is in a convergent state. But this would imply that the computation may proceed via a σ move.

Now suppose that for some $m \geq 0$ $SBarb(p)$ contains a barb $\underline{a_n} = s_1S_1'\sigma s_2S_2'\sigma s_3 ... s_n'\Omega$, with $n < m$ and s_n' a prefix of s_n, which satisfies $\underline{a_n} \ll \underline{b_n}$. Then this would lead to a derivation from p of the form

$$p = p_0 \overset{s_1}{\Longrightarrow} g_1 \xrightarrow{\sigma} \overset{s_2}{\Longrightarrow} \ldots \overset{s_n}{\Longrightarrow} g_n$$

where $S(g_i) = S_i'$ for $i < n$ and $g_n \Uparrow$. This could be zipped together with the derivation from e in (3) to obtain a computation from $e|p$, which only uses the test states e_0, e_1, e_2,...

$$e|p \mapsto e_1|p_1 \mapsto \ldots \mapsto e_l|p_l = e_l|g_n \xrightarrow{\tau} e_l|g_{n+1} \xrightarrow{\tau} \ldots$$

which will either be infinite or terminate at some $e_l|g_{n+j}$ with $g_{n+j} \uparrow$ depending on why $g_n \Uparrow$.

Since p *must* e it follows that for some e_i, $e_i \xrightarrow{\omega}$. Therefore the original computation (1) is successful. We know that the zipping together of these derivations works because at each state where the $\mapsto$ move is the result of a σ action the relevant S'_i is contained in S_i.

So we may assume that $SBarb(p)$ does not contain any such open barbs. It follows that the origional computation (1) and the sequence of barbs $\underline{b_1}, \underline{b_2} \ldots$ are infinite; a maximal barb b_m would be open and since $p \ll q$ $SBarb(p)$ would have to contain an $\underline{a}$ such that $\underline{a} \ll \underline{b_k}$ and neccessarily $\underline{a}$ would be open.

So let us consider the infinite sequence of barbs $\underline{b_1}, \underline{b_2} \ldots$. For each $\underline{b_k}$ we can obtain a barb of p of the form $\underline{a_k} = s_1 S'_1 \sigma s_2 S'_2 \sigma s_3 \ldots s_k S'_k$ with $s'_i \subseteq S(r_i)$ for each $1 \leq i \leq k$. This gives us the following dervation from p.

$$p = p_0 \overset{s_1}{\Longrightarrow} g_1 \xrightarrow{\sigma} \overset{s_2}{\Longrightarrow} \ldots \overset{s_k}{\Longrightarrow} g_k$$

where $S(g_i) = S'_i$ for $1 \leq i \leq k$. From this we wish to deduce the existence of an infinite derivation from p

$$p = p_0 \overset{s_1}{\Longrightarrow} g_1 \xrightarrow{\sigma} \overset{s_2}{\Longrightarrow} \ldots \xrightarrow{\sigma} \overset{s_k}{\Longrightarrow} g_k \ldots . \tag{4}$$

However this requires the assumption that the transition system generated by p, based on the "weak moves" $\overset{\lambda}{\Longrightarrow}$, is finite branching. For if it were not, p may have a branch to match each of these barbs while having no infinite branch to match them all. To prove this assumption true we can show that, in the terminology of [Ab90], it is weakly finite branching – that is for each q accessible from p $\{p' : \exists \mu . q \xrightarrow{\mu} p'\}$ is finite – and also that $\{p' : q \xrightarrow{\tau}^* p'\}$ is finite. The proof depends on the fact that $q \downarrow$ for each such q and is very similar to the corresponding proof in [dNH84] and is therefore omitted.

The derivation (4) can be combined with the computation from e in (3) to obtain an infinite computation from $e|p$ which only uses the test states e_0, e_1, ... Again, using p *must* e we can conclude that the original computation (1) is successful.

This leaves the case when some $e_n \uparrow$, which we leave to the reader. It is sufficient to consider the barb from $SBarb(q)$ which characterises the contribution of q up to the appearance of e_n and use the corresponding barb from p to obtain some e_k with $k \leq n$ and $e_k \xrightarrow{\omega}$. $\square$

We prove the converse by showing that in some sense the ability to generate a particular barb may be captured by an associated test. For every barb $\underline{b}$ and finite set of actions L define the test $e(\underline{b}, L)$ by induction on $\underline{b}$ as follows:

1. $e(\Omega, L) = \tau.\omega$
2. $e(A, L) = \lfloor \sum_{x \in L \setminus A} x.\omega \rfloor (nil)$
3. $e(c\underline{b'}, L) = \tau.\omega + \overline{c}.e(\underline{b'}, L)$
4. $e(A\sigma\underline{b'}, L) = \lfloor \sum_{x \in L \setminus A} x.\omega \rfloor (e(\underline{b'}, L))$

We leave the reader to check the following property of these tests:

Lemma 3.7 *For every standard barb $\underline{b}$ and for every finite $L \subseteq Act$ such that $Sort(\underline{b}) \subseteq L$ if $Sort(p) \subseteq L$ then*

$$p \ \not{m}ust \ e(\underline{b}, L) \Leftrightarrow \exists \underline{a} \in SBarb(p) \ \ \underline{a} \ll \underline{b}.$$

Proposition 3.8 *For p,q in TPL $p \underset{\sim}{\sqsubset} q$ implies $p \ll q$.*

Proof: We prove the contrapositive, namely $\neg(p \ll q)$ implies $\neg(p \underset{\sim}{\sqsubset} q)$. If $p \ll q$ is not true then for some standard barb $\underline{b} \in SBarb(q)$ $\underline{b}' \ll \underline{b}$ for no $\underline{b}'$ in $SBarb(p)$. In this case we employ the Lemma 3.7 where L is chosen so as to contain both of the finite sets $Sort(p)$ and $Sort(q)$. □

Combining these two propositions we immediately have the Alternative Characterisation Theorem for *TPL*. As a direct corollary to this we can restrict the experimenters considered with no change to the discriminatory power.

Definition 3.9 An *F-test* f is a *TPL* experiment of the following recursively defined form.

- $f = \tau.\omega$.
- $f = \lfloor \sum_A a.\omega \rfloor (nil)$.
- $f = \tau.\omega + a.f'$, where f' is an F-test.
- $f = \lfloor \sum_A a.\omega \rfloor (f')$, where f' is an F-test.

□

Lemma 3.10 *For any TPL processes p,q $p \underset{\sim}{\sqsubset} q$ if, and only if, for all F-tests f p must f implies q must f*

Proof: We have proved above that $p \underset{\sim}{\sqsubset} q \ \Leftrightarrow \ p \ll q$. The proof of Lemma 3.7 then gives that we need only consider F-tests. □

With this alternative characterisation it is now relatively straightforward to compare processes with respect to $\underset{\sim}{\sqsubset}$. As an example we return to Example 2.7. We can distinguish the two vending machines with the barb $coin\{tea, hit\}\sigma hit\{tea\}$ which is a standard barb of the second process unmatched by one from the first. The alternative characterisation also enables us to prove the characterisation of $\underset{\sim}{\sqsubset}^c$ promised in the previous section.

Theorem 3.11

$$p \underset{\sim}{\sqsubset}^c q \ \ \Leftrightarrow p \underset{\sim}{\sqsubset}^+ q.$$

Proof: It is sufficient to show that $\underset{\sim}{\sqsubset}^+$ is respected by all the operators. We leave the individual proofs, which are quite tedious to the reader but we should point out the proof for the restriction operator requires some care. □

4 Proof Systems

In this section we develop a sound and complete proof system for the language *TPL*. The importance of a proof system for a language is great. Some process algebras are defined equationally since their designers feel this to be the most intuitive starting point. Indeed Schmidt says in [Sch86]:

> "The [axiomatic] format is best used to provide preliminary specifications for a language or to give documentation about properties that are of interest to the users of the language."

Hence it is often to the equations that one turns to reveal the differences between languages and the equivalences defined upon them. The importance of the soundness of a proof system is obvious, it merely requires that the equations and proof rules are true of the language under examination. Completeness is often harder to prove since it requires that all truths in the language should be provable in the proof system.

The proof system we consider is based on the inequations given in Figures 4 and 5. Many of these are standard equations for *CCS* but the operators $\lfloor\ \rfloor(\ )$ and σ introduce new and sometimes complex axioms, particularly in relation to the internal operator τ. From the equation $\sigma 1$ it is apparent that σ is expressible in terms of $\lfloor\ \rfloor(\ )$ but we have deliberately used σ in the presentation because it is easily understood intuitively. Also note that $e1$ is not derivable from $e2$.

The proof system is defined in Figure 6. It is essentially inequational reasoning with extra rules for recursive terms, *REC* and $\omega - Induction$. In the latter $App(t)$ denotes the set of finite approximations to t, $\{t^n : n \geq 0\}$, defined by:

1. $t^0 = \Omega$
2. (a) $x^{n+1} = x$
   (b) $f(\underline{t})^{n+1} = f(\underline{t}^{n+1})$
   (c) $(recx.t)^{n+1} = t^{n+1}[(recx.t)^n/x]$.

These have been discussed at length in [He88]. The only extra rule is the $Stability-Rule$, a simple form of which equates the process $a.nil$ with $recx.(a.nil + \sigma.x)$ or even nil with $recx.\sigma.x$.

Let $\vdash_E t \leq u$ denote that $t \leq u$ is derivable in this proof system, $t \leq_E u$ that $t \leq u$ is derivable with purely inequational reasoning and finally $t \leq_{Er} u$ that $t \leq u$ is derivable using in addition the unfolding rule *REC*.

We first discuss the soundness of the axioms. To characterise their importance we introduce two further equivalences, derivation congruence and observational congruence, [Mil90].

Definition 4.1 *Derivation congruence* is the largest equivalence satisfying

$$< p, q > \in S \Rightarrow \begin{array}{ll} i) & \forall p'.p \xrightarrow{\lambda} p'.q \xrightarrow{\lambda} p' \\ ii) & p \Downarrow \Leftrightarrow q \Downarrow \end{array}$$

where $\lambda \in Act \cup \{\tau, \sigma\}$. □

$$\begin{array}{rcll@{\qquad}rcll}
x+x & = & x & +1 & \tau.x+x & = & \tau.x & \tau 1 \\
x+y & = & y+x & +2 & \tau.x+y & = & \tau.(\tau.x+y) & \tau 2 \\
x+(y+z) & = & (x+y)+z & +3 & a.x+a.y & = & a.(\tau.x+\tau.y) & \tau 3 \\
x+nil & = & x & +4 & \tau.x+y & \leq & \tau.x & \tau 4 \\
 & & & & \tau.x+\tau.y & \leq & \tau.(x+y) & \tau 5
\end{array}$$

$$\begin{array}{rcll@{\qquad}rcll}
nil \setminus a & = & nil & res1 & nil[S] & = & nil & rel1 \\
\alpha.x \setminus a & = & nil & res2 & (\alpha.x)[S] & = & S(\alpha).x[S] & rel2 \\
 & & \alpha \in \{a,\overline{a}\} & & & & & \\
\alpha.x \setminus a & = & \alpha.(x \setminus a) & res3 & (x+y)[S] & = & x[S]+y[S] & rel3 \\
 & & \alpha \notin \{a,\overline{a}\} & & & & & \\
(x+y) \setminus a & = & x \setminus a + y \setminus a & res4 & & & & \\
\lfloor x \rfloor (y) \setminus a & = & \lfloor x \setminus a \rfloor (y \setminus a) & res5 & \lfloor x \rfloor (y)[S] & = & \lfloor x[S] \rfloor (y[S]) & rel4
\end{array}$$

$$\begin{array}{rcll@{\qquad}rcll}
\tau.\Omega & = & \Omega & \Omega 1 & \Omega \setminus a & = & \Omega & \Omega 4 \\
x+\Omega & = & \Omega & \Omega 2 & \Omega[S] & = & \Omega & \Omega 5 \\
x|\Omega & = & \Omega & \Omega 3 & \lfloor \Omega \rfloor (x) & = & \Omega & \Omega 6
\end{array}$$

Figure 4: The Inequation System E

We write $p \sim q$ to say that p and q are derivation congruent.

Definition 4.2 *Observational equivalence* is the largest equivalence satisfying

$$< p,q > \in S \Rightarrow \begin{array}{ll} i) & \forall p'.p \overset{\lambda}{\Longrightarrow} p'.\exists q'.q \overset{\lambda}{\Longrightarrow} q'. < p',q' > \in S \\ ii) & p \Downarrow \Leftrightarrow q \Downarrow \end{array}$$

where $\lambda \in Act \cup \{\sigma, \varepsilon\}$. □

It is well known that $\approx$ is not preserved by $+$ ([Mil90]) but if, as usual, we define $p \approx^+ q$ if for some a not appearing in p or q $p+a \approx q+a$, then $\approx^+$ is a congruence with respect to all our operators.

$$\begin{aligned}
\sigma.x &= \lfloor nil \rfloor(x) && \sigma 1\\
a.x &= \lfloor a.x \rfloor(a.x) && \sigma 2\\
\lfloor \lfloor x \rfloor(y) \rfloor(z) &= \lfloor x \rfloor(z) && \sigma 3\\
\lfloor x \rfloor(y) + \lfloor u \rfloor(v) &= \lfloor x+u \rfloor(y+v) && \sigma 4
\end{aligned}$$

$$\begin{aligned}
\lfloor \tau.x \rfloor(y) &= \tau.x && \sigma\tau 1\\
\tau.\lfloor x \rfloor(y) &= \tau.\lfloor x \rfloor(\tau.y) && \sigma\tau 2\\
x + \tau.\lfloor y \rfloor(z) &\leq \tau.\lfloor x+y \rfloor(z) && \sigma\tau 3
\end{aligned}$$

$$\begin{aligned}
x = \textstyle\sum_I \mu_i.x_i \quad & \quad y = \textstyle\sum_J \gamma_j.y_j\\
x|y &= \textstyle\sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) + \sum_{\mu_i=\overline{\gamma_j}} \tau.(x_i|y_j) && e1
\end{aligned}$$

$$\begin{aligned}
x = \lfloor \textstyle\sum_I \mu_i.x_i \rfloor(x_\sigma) \quad & \quad y = \lfloor \textstyle\sum_J \gamma_j.y_j \rfloor(y_\sigma)\\
x|y &= \lfloor \textstyle\sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) + \sum_{\mu_i=\overline{\gamma_j}} \tau.(x_i|y_j) \rfloor(x_\sigma|y_\sigma) && e2
\end{aligned}$$

Figure 5: Extra Inequations for System E

Lemma 4.3 *For any TPL processes p and q*

$$p \sim q \;\Rightarrow\; p \approx q \;\Rightarrow\; p \lesssim q.$$

Proof: The first implication is straightforward and to show the second it is sufficient to prove prove that for any F-test f p $\not{m}ust$ f and $p \approx q$ implies q $\not{m}ust$ f by induction on the size of f. This we leave to the reader. □

We can now consider the soundness of most of our equations with respect to these congruences. The laws $+1, +2, +3$, and $+4$ are called the monoid laws (although commutativity idempotence is not required of monoids). In [Mil90] they are shown to be sound with respect to $\sim$. The equations $res1, res2, res3, res4, rel1, rel2, rel3$, and $e1$ are also discussed there. Note that this does not necessarily imply that these laws are sound over *TPL*. For example in [Mil90] $x + y \sim y + x$ follows since $x + y \xrightarrow{\alpha} z$ can only be the result of $x \xrightarrow{\alpha} z$ or $y \xrightarrow{\alpha} z$ but not both. We would also have to consider the case where $x \xrightarrow{\sigma} x'$ and $y \xrightarrow{\sigma} y'$ implying $x + y \xrightarrow{\sigma} x' + y'$. However these extra cases are straightforward to check.

We can justify many more of our equations in terms of derivation and observation congruence. The equations $\sigma 1, \ldots \sigma 4, \sigma\tau 1$ and $e2$ are all true of $\sim$. As examples we consider the two equations $\sigma 4$ and $e2$.

1. *Reflexivity* $$\frac{}{t \leq t}$$

2. *Transitivity* $$\frac{t \leq t',\ t' \leq t''}{t \leq t''}$$

3. *Substitution* (a) $$\frac{\underline{t} \leq \underline{t}'}{f(\underline{t}) \leq f(\underline{t}')}$$ *for every* $f \in \{\mu., +, |, \backslash a, [S]\}$

   (b) $$\frac{t \leq t'}{recx.t \leq recx.t'}$$

4. *Instantiation* $$\frac{t \leq t'}{t\rho \leq t'\rho}$$ *for every substitution* ρ

5. *Inequations* $$\frac{}{t \leq t'}$$ *for every inequation* $t \leq t'$ *in* E

6. $\Omega -$ *Rule* $$\frac{}{\Omega \leq t}$$

7. *REC* $$\frac{}{recx.t = t[recx.t/x]}$$

8. $\omega -$ *Induction* $$\frac{for\ every\ d \in App(t), d \leq t'}{t \leq t'}$$

9. *Stability* $-$ *Rule* $$\frac{}{\sum_{i \in I} \alpha_i.t_i \leq recx.\lfloor \sum_{i \in I} \alpha_i.t_i \rfloor(x)}$$ $\alpha_i \in Act_\tau$

Figure 6: The Proof System

- $\lfloor x \rfloor(y) + \lfloor u \rfloor(v) = \lfloor x + u \rfloor(y + v)$. Firstly we examine the σ transition possible if x and u cannot perform a τ move. $THEN_2$ gives $\lfloor x + u \rfloor(y + v) \xrightarrow{\sigma} y + v$. It also gives $\lfloor x \rfloor(y) \xrightarrow{\sigma} y$ and $\lfloor u \rfloor(v) \xrightarrow{\sigma} v$ so by SUM_3 the only available σ move from $\lfloor x \rfloor(y) + \lfloor u \rfloor(v)$ is $\lfloor x \rfloor(y) + \lfloor u \rfloor(v) \xrightarrow{\sigma} y + v$. The other transitions from $\lfloor x+u \rfloor(y+v)$ must, by $THEN_1$, come from $x+u$. By SUM_1 and SUM_2 these must be from $x \xrightarrow{\alpha} x'$ or $u \xrightarrow{\alpha} u'$ giving $\lfloor x + u \rfloor(y + v) \xrightarrow{\alpha} x'$ or $\lfloor x + u \rfloor(y + v) \xrightarrow{\alpha} y'$. Now the initial moves (i.e. non σ moves) of $\lfloor x \rfloor(y) + \lfloor u \rfloor(v)$ are derived from SUM_1 and SUM_2 i.e. from $\lfloor x \rfloor(y)$ and $\lfloor u \rfloor(v)$. $THEN_1$ gives these as the result of $x \xrightarrow{\alpha} x'$ or $u \xrightarrow{\alpha} u'$. So $\lfloor x \rfloor(y) + \lfloor u \rfloor(v) \xrightarrow{\alpha} x'$ or $\lfloor x \rfloor(y) + \lfloor u \rfloor(v) \xrightarrow{\alpha} u'$ as before.

- If $x = \lfloor \sum_I \mu_i.x_i \rfloor (x_\sigma)$ and $y = \lfloor \sum_J \gamma_j.y_j \rfloor (y_\sigma)$ then $x|y = \lfloor \sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) + \sum_{\mu_i = \overline{\gamma_j}} \tau.(x_i|y_j) \rfloor (x_\sigma | y_\sigma)$. We examine wait transitions first. For the left hand side these can only be the result of COM_4 which can only be applied when $x \xrightarrow{\sigma} x'$, $y \xrightarrow{\sigma} y'$ and $x|y \not\xrightarrow{\tau}$. $THEN_2$ translates this first two conditions into $\tau \notin (\{\mu_i : i \in I\} \cup \{\gamma_j : j \in J\})$ giving $x \xrightarrow{\sigma} x_\sigma$ and $y \xrightarrow{\sigma} y_\sigma$. The third condition implies (by COM_3) that $\{\mu_i : i \in I\} \cap \{\overline{\gamma_j} : j \in J\} = \emptyset$. These conditions also imply $\lfloor \sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) + \sum_{\mu_i = \overline{\gamma_j}} \tau.(x_i|y_j) \rfloor (x_\sigma | y_\sigma)$ is $\lfloor \sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) \rfloor (x_\sigma | y_\sigma)$ and by $THEN_2$ we have $\lfloor \sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) \rfloor (x_\sigma | y_\sigma) \xrightarrow{\sigma} x_\sigma | y_\sigma$. The other moves are derived for the left hand side by COM_1, COM_2, and COM_3 and for the right hand side by $THEN_1$. We examine only one case in detail. Suppose $x|y \xrightarrow{a} x_a|y$ by COM_1. Then by repeated use of SUM_1 we have $\sum_I \mu_i.(x_i|y) + \sum_J \gamma_j.(x|y_j) + \sum_{\mu_i = \overline{\gamma_j}} \tau.(x_i|y_j) \xrightarrow{a} x_a|y$. $THEN_1$ then gives desired move from the right.

The axioms $\tau 1$, $\tau\sigma 2$, $\Omega 1$, $\Omega 4$, and $\Omega 5$ are all true of observational congruence. The only non-trivial axiom to check is $\tau\sigma 2$ which relates the congruence to stability: for any two processes p, q $\tau.\lfloor p \rfloor (q)$ and $\tau.\lfloor p \rfloor (\tau.q)$ are obviously observationally equivalent because $\lfloor p \rfloor (q)$ and $\lfloor p \rfloor (\tau.q)$ are observationally equivalent and the extra condition for congruence is easily checked. The standard τ-laws of *CCS* may also be derived from ours. $\tau 1$ is the second τ-law of *CCS* (see for example [Mil90]). The first τ-law, $\alpha.\tau.x = \alpha.x$, follows from our $\tau 2$ (with $y = \tau.x$) and $\tau 3$ (with $y = x$). The third, $\alpha.(x + \tau.y) + \alpha.y = \alpha.(x + \tau.y)$ is derivable as follows:

$$\begin{array}{rcll} \alpha.(x+\tau.y)+\alpha.y & = & \alpha.(\tau.(x+\tau.y)+\tau.y) & \tau 3 \\ & = & \alpha.(x+\tau.y+\tau.y) & \tau 2 \\ & = & \alpha.(x+\tau.y) & +1. \end{array}$$

The remaining equations $\tau 2$, $\tau 3$, $\tau 4$, $\tau 5$, $\sigma\tau 3$, $\Omega 2$, and $\Omega 3$ have to be justified directly in terms of $\ll^c$. We look at two examples:

- $\tau.x + \tau.y \leq \tau.(x + y)$. This is not straightforward, but it embodies the idea that nondeterminism is decreased as one moves up the preorder. We prove this sound by induction on the length of barbs.
  - $\Omega \in SBarb(\tau.(x + y))$. Then $(x + y) \Uparrow$ and so either $x \Uparrow$ or $y \Uparrow$ and so $(\tau.x + \tau.y) \Uparrow$ and $\Omega \in SBarb(\tau.x + \tau.y)$.
  - $A \in SBarb(\tau.(x + y))$. Then either $x \overset{\varepsilon}{\Longrightarrow} x'$ with $A = S(x')$, $y \overset{\varepsilon}{\Longrightarrow} y'$ with $A = S(y')$, or $A = S(x) \cup S(y)$. In either case this can be matched by $\tau.x + \tau.y$.
  - $a\underline{b} \in SBarb(\tau.(x + y))$. Then $\tau.(x + y) \overset{a}{\Longrightarrow} z$ with $\underline{b} \in SBarb(z)$. But then either $x \overset{a}{\Longrightarrow} z$ or $y \overset{a}{\Longrightarrow} z$ and so $a\underline{b} \in SBarb(\tau.x + \tau.y)$.
  - $A\sigma\underline{b} \in SBarb(\tau.(x + y))$. Now if either $A\sigma\underline{b} \in SBarb(x)$ or $A\sigma\underline{b} \in SBarb(y)$ we have $A\sigma\underline{b} \in SBarb(\tau.x + \tau.y)$. Suppose not, that is $x \xrightarrow{\sigma} x'$ and $y \xrightarrow{\sigma} y'$ with $A = S(x) \cup S(y)$ and $\underline{b} \in SBarb(x' + y')$. Then $\underline{b} \in SBarb(\tau.(x' + y'))$ and so by induction $\underline{a} \in SBarb(\tau.x' + \tau.y')$ with $\underline{a} \ll \underline{b}$. But $SBarb(\tau.x' + \tau.y') = SBarb(x') \cup SBarb(y')$ and so $\underline{a} \in SBarb(x')$ or $\underline{a} \in SBarb(y')$. Without loss of generality assume $\underline{a} \in SBarb(x')$. Then $S(x)\sigma\underline{a} \in SBarb(x) \subseteq SBarb(\tau.x + \tau.y)$ as required.

- $x + \tau.\lfloor y \rfloor(z) \leq \tau.\lfloor x + y \rfloor(z)$. We examine $\underline{b} \in SBarb(\tau.\lfloor x + y \rfloor(z))$. If $\underline{b} = \Omega$ then either $x \Uparrow$ or $y \Uparrow$ giving $(x + \tau.\lfloor y \rfloor(z)) \Uparrow$ and $\Omega \in SBarb(x + \tau.\lfloor y \rfloor(z))$. If $\underline{b} = a\underline{b}'$ then either $x \xrightarrow{a} x'$ with $\underline{b}' \in SBarb(x')$ or $y \xrightarrow{a} y'$ with $\underline{b}' \in SBarb(y')$. In either case $\underline{b} \in SBarb(x + \tau.\lfloor y \rfloor(z))$. Otherwise $\underline{b} = A\sigma\underline{b}'$. There are three cases to consider.
  - $x \overset{\tau}{\Longrightarrow} x'$ with $A = S(x')$ and $\underline{b} \in SBarb(x')$. Then $x + \tau.\lfloor y \rfloor(z) \overset{\tau}{\Longrightarrow} x'$ and $\underline{b} \in SBarb(x + \tau.\lfloor y \rfloor(z))$.
  - $y \overset{\tau}{\Longrightarrow} y'$ with $A = S(y')$ and $\underline{b} \in SBarb(y')$. Then $x + \tau.\lfloor y \rfloor(z) \overset{\tau}{\Longrightarrow} y'$ and $\underline{b} \in SBarb(x + \tau.\lfloor y \rfloor(z))$.
  - $A = S(x) \cup S(y)$ and $\underline{b}' \in SBarb(z)$. Then $S(y)\sigma\underline{b}' \in SBarb(x + \tau.\lfloor y \rfloor(z))$ with $S(y)\sigma\underline{b}' \ll A\sigma\underline{b}'$.

We have just shown:

Proposition 4.4 *All the inequations in Figures 4 and 5 are sound with respect to* $\sqsubseteq^c$.

At this point it is convenient to ignore the soundness of the proof system and instead address completeness.

In common with most completeness proofs in the process algebra literature we start by defining the notion of normal form. These are gleaned from the behavior of processes and the mechanics of the proof that every term indeed has a normal form. In the following definition of normal forms we make the distinction between stable and unstable processes. If the process is stable then either it changes under the passage of one unit of time or it does not. If the process is unstable then either it is divergent or it has a number of actions available to it before nondeterministicly resolving its instability in favour of a stable normal form.

Definition 4.5 A *normal form* (nf for short) is a term of the following inductively defined form.

1. Ω is a normal form.
2. $\lfloor \sum_A a.n_a \rfloor(n_\sigma)$ is a normal form if each n_a is a normal form and n_σ is a normal form.
3. $\sum_B b.n_b + \sum_I \tau.n_i$ is a normal form if each n_b is a normal form and each n_i is a stable normal form.

□

Taking I to be empty gives normal forms $\sum_A a.n_a$ and also taking A to be empty gives the normal form *nil*. It may also be worth clarifying the notation $\sum_X f(x)$. This is intended as a shorthand for $\sum_{x \in X} f(x)$. We will use and abuse this notation liberally. We also denote by n_a the unique m such that the normal form n can evolve to by performing an a action, i.e. $n \xrightarrow{a} m$.

In proving that every term can be reduced to a normal form we need a measure on which to perform induction.

Definition 4.6 The *depth* of a finite process d written $|d|$ is defined structurally as follows.

- $|\Omega| = |nil| = 0$.
- $|a.d| = 1 + |d|$.
- $|\tau.d| = |d|$.
- $|\sigma.d| = |d|$.
- $|d + e| = max\{|d|, |e|\}$.
- $|\lfloor d \rfloor (e)| = max\{|d|, |e|\}$.
- $|d|e| = |d| + |e|$.
- $|d \setminus a| = |d|$.
- $|d[S]| = |d|$.

□

The depth of a term is supposed to represent the maximum length of a trace from that term, ignoring τ and σ actions. To avoid complication $|d \setminus a|$ is defined as $|d|$ when obviously it could be much less. The reason for ignoring σ comes from the line $|\lfloor d \rfloor (e)| = max\{|d|, |e|\}$. If we replace this with the perhaps more intuitive $|\lfloor d \rfloor (e)| = max\{|d|, 1 + |e|\}$ (and adjust $|\sigma.d|$ accordingly) it is difficult to see how to construct a normal form from the choice between the two normal forms $\sum_A a.n_a$ and $\lfloor \sum_B b.m_b \rfloor (m_\sigma)$ without possibly *increasing* the overall depth. Normalisation will be performed using the following measure.

Definition 4.7 The measure $\prec$ is the preorder defined by

1. $|d| < |f|$ or
2. $|d| = |f|$ and $M_\sigma(d) < M_\sigma(f)$ where $M_\sigma(p)$ denotes the number of occurences of the constuct $\lfloor\ \rfloor(\ )$ in p.

We write $d \preceq f$ when either $d \prec f$ or $|d| = |f|$ and $M_\sigma(d) = M_\sigma(f)$, that is when neither the depth or M_σ are greater in d than f. □

The following fact is used repeatedly when normalising a finite term and so is dealt with separately.

Lemma 4.8 *For finite sets of normal forms $\{p_a : a \in A\}$ and $\{q_b : b \in B\}$ ($A, B \subseteq Act$) there exists normal forms r_c such that $\sum_A a.p_a + \sum_B b.q_b =_E \sum_{A \cup B} c.r_c$ and $\sum_{A \cup B} c.r_c \preceq \sum_A a.p_a + \sum_B b.q_b$.*

Proof: We first show by a case analysis on n that if n is a normal form then there exists a normal form n' such that

1. $n' =_E \tau.n$.

2. $n' \preceq n$.

This in turn is used to show that if n_1 and n_2 are normal forms then there exists a normal form n_3 such that

1. $n_3 =_E \tau.n_1 + \tau.n_2$.

2. $n_3 \preceq \tau.n_1 + \tau.n_2$.

This is proved by induction on the depth of $n_1 + n_2$. The proof of the result is now straightforward:

$$\begin{array}{lcll}
\sum_A a.p_a + \sum_B b.q_b & =_E & \sum_{A\backslash B} a.p_a + \sum_{B\backslash A} b.q_b + \sum_{A\cap B} c.(\tau.p_c + \tau.q_c) & \text{by } \tau 3 \\
\sum_A a.p_a + \sum_B b.q_b & =_E & \sum_{A\backslash B} a.p_a + \sum_{B\backslash A} b.q_b + \sum_{A\cap B} c.nf(\tau.p_c + \tau.q_c) & \text{by above}
\end{array}$$

□

Theorem 4.9 *(Normal Form Theorem)*
Every finite term p has an equationally equivalent normal form nf(p) with $nf(p) \preceq p$.

Proof:
We proceed by induction on $\preceq$. There are several cases to consider depending on the structure of p but we examine only $p + q$ here.

- $nf(p) =_E \lfloor \sum_A a.p_a \rfloor (p_\sigma)$, $nf(q) =_E \lfloor \sum_B b.q_b \rfloor (q_\sigma)$.

$$\begin{array}{rcll}
p + q & =_E & nf(p) + nf(q) & \text{by substitution} \\
 & =_E & \lfloor \sum_A a.p_a \rfloor (p_\sigma) + \lfloor \sum_B b.q_b \rfloor (q_\sigma) & \text{by substitution} \\
 & =_E & \lfloor \sum_A a.p_a + \sum_B b.q_b \rfloor (p_\sigma + q_\sigma) & \text{by } \sigma 4 \\
 & =_E & \lfloor \sum_A a.p_a + \sum_B b.q_b \rfloor (nf(p_\sigma + q_\sigma)) & \text{by induction on } \preceq
\end{array}$$

The result then follows by Lemma 4.8

- $nf(p) =_E \sum_A a.p_a$, $nf(q) =_E \lfloor \sum_B b.q_b \rfloor (q_\sigma)$.

$$\begin{array}{rcll}
p + q & =_E & nf(p) + nf(q) & \text{by substitution} \\
 & =_E & \sum_A a.p_a + \lfloor \sum_B b.q_b \rfloor (q_\sigma) & \text{by substitution} \\
 & =_E & \lfloor \sum_A a.p_a + \sum_B b.q_b \rfloor (\sum_A a.p_a + q_\sigma) & \text{by } \sigma 2 \ \& \ \sigma 4 \\
 & =_E & \lfloor \sum_A a.p_a + \sum_B b.q_b \rfloor (nf(\sum_A a.p_a + q_\sigma)) & \text{by induction on } \preceq
\end{array}$$

The result then follows as above by Lemma 4.8.

- $nf(p) =_E \lfloor \sum_A a.p_a \rfloor (p_\sigma)$, $nf(q) =_E \sum_B b.q_b + \sum_{J \neq \emptyset} \tau.q_j$.

$$\begin{array}{rcll}
p + q & =_E & nf(p) + nf(q) & \text{by substitution} \\
 & =_E & \lfloor \sum_A a.p_a \rfloor (p_\sigma) + \sum_B b.q_b + \sum_{J \neq \emptyset} \tau.q_j & \text{by substitution} \\
 & =_E & \sum_A a.p_a + \sum_B b.q_b + \sum_{J \neq \emptyset} \tau.q_j & \text{by } \sigma\tau 3
\end{array}$$

Again the result follows from Lemma 4.8.

- $nf(p) =_E \sum_A a.p_a + \sum_I \tau.p_i$, $nf(q) =_E \sum_B b.q_b + \sum_J \tau.q_j$.

$$\begin{array}{lll} p+q & =_E \; nf(p)+nf(q) & \text{by substitution} \\ & =_E \; \sum_A a.p_a + \sum_{I\neq\emptyset} \tau.p_i + \sum_B b.q_b + \sum_{J\neq\emptyset} \tau.q_j & \text{by substitution} \end{array}$$

The result follows as before from Lemma 4.8.

□

It will be convenient in the completeness theorem to be able to further reduce normal forms. These we call *strong normal forms.*

Definition 4.10 A normal form with the structure $\sum_A a.d_a + \sum_{I\neq\emptyset} \tau.d'_i$ where each d_i is a stable normal form (i.e. $\sum_{B_i} b.d^i_b$ or $\lfloor \sum_{B_i} b.d^i_b \rfloor (d^i_\sigma)$) is a *strong normal form* if

1. each B_i is contained in A and
2. for each a in $A \cap B_i$, $\tau.d_a + \tau.d^i_a =_E d_a$.

□

We use $snf(d)$ to denote the strong normal form of a term d. We did not include this information in the definition of normal forms as the translation of a τ-stable process into its associated strong normal form may *increase* the depth of the term. However we can prove the following lemma.

Lemma 4.11 *For every normal form $d = \sum_A a.d_a + \sum_{I\neq\emptyset} \tau.d_i$ with $d_i = \sum_{B_i} b.d^i_b$ or $d_i = \lfloor \sum_{B_i} b.d^i_b \rfloor (d^i_\sigma)$ there exists a strong normal form $snf(d) = \sum_{A'} a.d'_a + \sum_{I\neq\emptyset} \tau.d_i$ such that $d =_E snf(d)$ and $d'_a \prec d$.*

Proof: We proceed by direct equational manipulation of d. We will use the derived axiom $\tau.\lfloor x \rfloor (y) = x + \tau.\lfloor x \rfloor (y)$. (This follows from $\tau 1$ and the easily derivable equation $\lfloor x \rfloor (y) + \tau.z = x + \tau.z$)

$$\begin{array}{lll} d & =_E \; \sum_A a.d_a + \sum_{I\neq\emptyset} \tau.d_i & \text{by def}^{\underline{n}} \\ & =_E \; \sum_A a.d_a + \sum_J \tau.\sum_{B_j} b.d^j_b + \sum_K \tau.\lfloor \sum_{B_k} b.d^k_b \rfloor (d^k_\sigma) & \text{by def}^{\underline{n}} \\ & =_E \; \sum_A a.d_a + \sum_J \sum_{B_j} b.d^j_b + \sum_J \tau.\sum_{B_j} b.d^j_b + \sum_K \tau.\lfloor \sum_{B_k} b.d^k_b \rfloor (d^k_\sigma) & \text{by} \tau 1 \\ & =_E \; \sum_A a.d_a + \sum_J \sum_{B_j} b.d^j_b + \sum_K \sum_{B_k} b.d^k_b + \sum_J \tau.\sum_{B_j} b.d^j_b + \sum_K \tau.\lfloor \sum_{B_k} b.d^k_b \rfloor (d^k_\sigma) & \\ & & \text{from above} \\ & =_E \; \sum_A a.d_a + \sum_J \sum_{B_j} b.d^j_b + \sum_K \sum_{B_k} b.d^k_b + \sum_{I\neq\emptyset} \tau.d_i & \text{by def}^{\underline{n}} \end{array}$$

We now examine the term $\sum_A a.d_a + \sum_J \sum_{B_j} b.d^j_b + \sum_K \sum_{B_k} b.d^k_b$ in isolation: we aim to translate it into the form $\sum_{A'} a.d'_a$. Suppose $a.d_1$ and $a.d_2$ are both summands of $\sum_A a.d_a + \sum_J \sum_{B_j} b.d^j_b + \sum_K \sum_{B_k} b.d^k_b$. Then by $\tau 3$ we have $a.d_1 + a.d_2 =_E a.(\tau.d_1 + \tau.d_2)$.As in Lemma 4.8 we can transform $a.d_1 + a.d_2$ into $a.nf(\tau.d_1 + \tau.d_2)$ with no increase in depth. We repeat this proceedure until no such duplicated prefixed action appear in the sum. It is then straightforward to check that the transformation of d is both a strong normal form and satisfies the requirements of the lemma. $\square$

It is also necessary to develop a partial normal form for infinite terms, i.e. those involving recursion. These are called head normal forms.

Definition 4.12 A *head normal form* is a term of the following form.

1. $\lfloor \sum_A a.p_a \rfloor (p_\sigma)$ is in head normal form.
2. $\sum_A a.p_a + \sum_{I \neq \emptyset} \tau.p_i$ is in head normal form if each p_i is in a stable head normal form.

$\square$

We use $hnf(p)$ to denote the head normal form of a term p.

Theorem 4.13 *(Head Normal Form Theorem)*
For any term p such that $p \Downarrow$ there exists a head normal form $hnf(p)$ such that $p =_{Er} hnf(p)$.

Proof: The proof is similar to that of the Normal Form Theorem except that the induction used is on the length of the proof that $p \Downarrow$. $\square$

In the next theorem, the heart of the completeness theorem, we use various simple facts about $\sqsubseteq^c$ which are summarised in the following lemma. The proofs are straightforward and are left to the reader.

Lemma 4.14

1. *(τ-preservation) $p \ll q \;\Rightarrow\; \tau.p \ll^c \tau.q$*
2. *(stability) for convergent p $p \ll^c q \wedge p \xrightarrow{\tau} \;\Rightarrow\; q \xrightarrow{\tau}$*
3. *(σ-property)*

$$\left.\begin{array}{c} p \ll^c q \\ p \xrightarrow{\sigma} p_\sigma \\ q \xrightarrow{\sigma} q_\sigma \end{array}\right\} \Rightarrow p_\sigma \ll^c q_\sigma .$$

Theorem 4.15 *(Partial Completeness) For any finite process d and any process q*

$$d \sqsubseteq^c q \;\Rightarrow \vdash_E d \leq q$$

Proof: We proceed by induction on the order $\prec$ over d and its subterms. For convenience we abbreviate $\vdash_E d \leq q$ to $d \leq_E q$ within the confines of this proof although essential use is made of the extra rules. We may assume d is in normal form. If $d \Uparrow$ then it is easy to prove by structural induction on d that $d =_E \Omega$ and the result follows immediately. So we may further assume that $d \Downarrow$ and therefore $q \Downarrow$; in particular we may now assume q is in head normal form.

- $d \equiv \lfloor \sum_A a.d_a \rfloor (d_\sigma), \quad q \equiv \lfloor \sum_B b.q_b \rfloor (q_\sigma)$

  Firstly we prove that $n_\sigma \leq_E q_\sigma$. $d_\sigma \ll^c q_\sigma$ follows directly from the σ-property, Part 3 of Lemma 4.14 and so by induction we have $d_\sigma \leq_E q_\sigma$.

  Now we prove $\sum_A a.d_a \leq_E \sum_B b.q_b$. Any barb $b\underline{v} \in SBarb(q)$ must be matched by one in $SBarb(d)$ so $B \subseteq A$. Any barb $B\sigma\underline{v} \in SBarb(q)$ must be matched by one in $SBarb(d)$ so $A \subseteq B$ i.e. $A = B$. Also for all $a \in A \;\; d_a \ll q_a$. For consider $\underline{v} \in SBarb(q_a)$. Then $a\underline{v} \in SBarb(q)$ and so by $d \ll^c q$ we have $a\underline{u} \in SBarb(d)$ with $a\underline{u} \ll a\underline{v}$. Hence $\underline{u} \ll \underline{v}$ with $\underline{u} \in SBarb(d_a)$. By the τ-preservation propery, Part 1 of Lemma 4.14 $d_a \ll q_a \quad \Rightarrow \quad \tau.d_a \ll^c \tau.q_a$ and so by induction for all $a \in A \; \tau.d_a \leq_E \tau.q_a$. Hence for all $a \in A \; a.\tau.d_a \leq_E a.\tau.q_a$ and so $\sum_A a.\tau.d_a \leq_E \sum_A a.\tau.q_a$ which, by $\tau 3$ gives $\sum_A a.d_a \leq_E \sum_A a.q_a$, i.e. $\sum_A a.d_a \leq_E \sum_B b.q_b$.

  Combining these results we have

$$d \equiv \lfloor \sum_A a.d_a \rfloor (d_\sigma) \leq_E \lfloor \sum_B b.q_b \rfloor (q_\sigma) \equiv q.$$

- $d \equiv \sum_B b.d_b + \sum_I \tau.d_i$.

  There are several sub-cases to consider.

  - $I = \emptyset$ i.e. $d \equiv \sum_A a.d_a$.

    Note that this includes the case when $A = \emptyset$, that is $d \equiv nil$. We define the term $e = recx.\lfloor \sum_A a.d_a \rfloor (x)$ and prove

$$\forall n. \forall p. d \ll^c p \;\Rightarrow e^n \leq_E p.$$

    We continue in this subproof by induction on n.

    * $n = 0$. $e^0 = \Omega$ and so by the $\Omega - Rule$ we have $e^0 \leq_E p$.
    * $n = k + 1$. By d's stability we know that p has the stable head normal form $p =_E \lfloor \sum_B b.p_b \rfloor (p_\sigma)$. First note that $d \ll^c p_\sigma$ follows directly by the σ-property and by induction on n we have $e^k \leq_E p_\sigma$.
      Now we prove that $\sum_A a.d_a \leq_E \sum_B b.p_b$. Any barb $b\underline{v} \in SBarb(p)$ must be matched by one in $SBarb(d)$ so $B \subseteq A$. Any barb $B\sigma\underline{v} \in SBarb(p)$ must be matched by one in $SBarb(d)$ so $A \subseteq B$ i.e. $A = B$. Also for all $a \in A \;\; d_a \ll p_a$. For consider $\underline{v} \in SBarb(p_a)$. Then $a\underline{v} \in SBarb(p)$ and so by $d \ll^c p$ we have $a\underline{u} \in SBarb(d)$ with $a\underline{u} \ll a\underline{v}$. Hence $\underline{u} \ll \underline{v}$ with $\underline{u} \in SBarb(d_a)$. By τ-preservation $d_a \ll p_a \quad \Rightarrow \quad \tau.d_a \ll^c \tau.p_a$ and so by induction for all $a \in A \; \tau.d_a \leq_E \tau.p_a$. Hence for all $a \in A \; a.\tau.d_a \leq_E a.\tau.p_a$ and so $\sum_A a.\tau.d_a \leq_E \sum_A a.\tau.p_a$ which, by $\tau 3$, gives $\sum_A a.d_a \leq_E \sum_A a.p_a$, i.e. $\sum_A a.d_a \leq_E \sum_B b.p_b$.
      Combining these results we obtain $\lfloor \sum_A a.d_a \rfloor (e^k) \leq_E \lfloor \sum_B b.p_b \rfloor (p_\sigma)$. But $e^{k+1} = \lfloor \sum_A a.d_a \rfloor (e^k)$ and so $e^{k+1} \leq_E p$ as required.

    Instantiating the p above to be the q of this theorem we have $\forall n. e^n \leq_E q$ and by $\omega - Induction$ we get $e \leq_E q$. By the $Stability - Rule$ $d \leq_E e$ and so $d \leq_E q$ as required.

– $I \neq \emptyset$.
This last case is the most complicated and we will go through it in some detail. Here d is an unstable normal form and therefore by Lemma 4.11 we may assume d is a strong normal form.

$$d \equiv \sum_A a.d_a + \sum_{I\neq\emptyset} \tau.d_i$$

$$\text{where} \quad d_i = \begin{cases} \sum_{B_i} b.d^i_b \text{ or} \\ \lfloor \sum_{B_i} b.d^i_b \rfloor (d_\sigma) \end{cases}$$

with for each B_i we have $B_i \subseteq A$ and $\tau.d_a + \tau.d^i_a =_E \tau.d^i_a$ for any $a \in B_i \cap A$. Further by the stability property, Part 2 of Lemma 4.14, we may assume that

$$q \equiv \sum_C c.q_c + \sum_{J\neq\emptyset} \tau.\lfloor \sum_{E_j} e.q^j_e \rfloor (q^j_\sigma).$$

First let us concentrate on the terms $c.q_c$. It is easy to establish that $C \subseteq A$ and for each c in C $d_c \ll q_c$ and therefore from τ-preservation $\tau.d_c \ll^c \tau.q_c$. By induction we have $\tau.d_c \leq_E \tau.q_c$ and therefore $c.d_c \leq_E c.q_c$. This means that for each such c $d \leq_E d + c.q_c$ and, because of $\tau 4$, to complete the theorem it is sufficient to prove $d \leq_E d + \tau.\lfloor \sum_{E_j} e.q^j_e \rfloor (q^j_\sigma)$ for each j in J. Let a typical such q^j be of the form $\lfloor \sum_E e.q_e \rfloor (q_\sigma)$. We actually show that $d' \leq_E \tau.\lfloor \sum_{E_j} e.q^j_e \rfloor (q^j_\sigma)$, where d' is $\sum_E e.d_e + \sum_{I'} \tau.d_i$ with $I' = \{i \in I : B_i \subseteq E\}$. Since $d \ll^+ q$ it follows that I' is not empty. We use induction on its size.

* $|I'| = 1$. Exactly how we proceed depends on the form of d'; it has either the form $\sum_E e.d_e + \tau.\sum_B b.d^1_b$ or $\sum_E e.d_e + \tau.\lfloor \sum_B b.d^1_b \rfloor (d^1_\sigma)$. We only consider the latter case in detail as the former is dealt with in a similar manner to the case above when $d = \sum_B b.d_b$.
We first show that $d^1_\sigma \ll q_\sigma$. To any barb $\underline{b} \in SBarb(q_\sigma)$ there corresponds a barb $E\sigma\underline{b} \in SBarb(q)$. This must be matched by a barb from d and the only candidates are those of the form $B\sigma\underline{b}'$ where $\underline{b}' \in SBarb(d^1_\sigma)$. Now by τ-preservation we have $\tau.d^1_\sigma \ll^c \tau.q_\sigma$ and therefore by induction $\tau.d^1_\sigma \leq_E \tau.q_\sigma$.
It is also easy to establish that $d_e \ll q_e$, by considering the possible barbs of q_e and using the fact that d is a strong normal form. Again using τ-preservation we have $d_e \leq_E q_e$ for each $e \in E$.
We now have the required ingredients to prove $d' \leq_E \tau.\lfloor \sum_E e.q_e \rfloor (q_\sigma)$:

$$\begin{array}{lll} \sum_E e.d_e + \tau.\lfloor \sum_B b.d^1_b \rfloor (d^1_\sigma) & & \\ \leq_E \quad \tau.\lfloor \sum_E e.d_e + \sum_B b.d^1_b \rfloor (d^1_\sigma) & & \text{by } \sigma\tau 3 \\ \leq_E \quad \tau.\lfloor \sum_E e.d_e \rfloor (d^1_\sigma) & & \text{by } \tau 3, \tau 4 \text{ since } B \subseteq E \\ =_E \quad \tau.\lfloor \sum_E e.d_e \rfloor (\tau.d^1_\sigma) & & \text{by } \sigma\tau 2 \\ \leq_E \quad \tau.\lfloor \sum_E e.q_e \rfloor (\tau.q_\sigma) & & \\ =_E \quad \tau.\lfloor \sum_E e.q_e \rfloor (q_\sigma) & & \text{by } \sigma\tau 2 \end{array}$$

This ends the proof when $|I'| = 1$.

* $|I'| > 1$.
  We suppose without loss of generality that $I' = \{1, 2, 3, ..., k\}$. We define a new term d'' which is a term lying between d' and $\tau.q_j$.

  $$d'' \equiv \sum_E e.d'_e + \sum_{2 \leq i \leq k} \tau.d'_i$$

  where for $3 \leq i \leq k$ we define $d'_i \equiv d_i$. The definition of d'_2 depends on the structure of d_1 and d_2 as does the rest of the proof.

  · $d_1 = \sum_{B_1} b.d^1_b \quad d_2 = \sum_{B_2} b.d^2_b$
    In this case we define:

    $$d'_2 \equiv \sum_{B_1 \setminus B_2} b.d^1_b + \sum_{B_2 \setminus B_1} b.d^2_b + \sum_{B_1 \cap B_2} b.nf(\tau.b^1_b + \tau.b^2_b).$$

    Then since $B_1 \cup B_2 \subseteq E$ we have $d'' \ll^c \tau.q_j$ and by induction $d'' \leq_E \tau.q_j$ as required.

  · $d_1 = \sum_{B_1} b.d^1_b \quad d_2 = \lfloor \sum_{B_2} b.d^2_b \rfloor (d^2_\sigma)$
    In this case we define:

    $$d'_2 \equiv \lfloor \sum_{B_1 \setminus B_2} b.d^1_b + \sum_{B_2 \setminus B_1} b.d^2_b + \sum_{B_1 \cap B_2} b.nf(\tau.b^1_b + \tau.b^2_b) \rfloor (nf(\tau. \sum_{B_1} b.d^1_b + \tau.d^2_\sigma)).$$

    Again $d'' \ll^c \tau.q_j$ and by induction $d'' \leq_E \tau.q_j$. By $\sigma 2$ and $\sigma\tau 2$ $d' \leq_E d''$ and so $d' \leq_E \tau.q_j$ as required.

  · $d_1 = \lfloor \sum_{B_1} b.d^1_b \rfloor (d^1_\sigma) \quad d_2 = \lfloor \sum_{B_2} b.d^2_b \rfloor (d^2_\sigma)$
    In this case we define:

    $$d'_2 \equiv \lfloor \sum_{B_1 \setminus B_2} b.d^1_b + \sum_{B_2 \setminus B_1} b.d^2_b + \sum_{B_1 \cap B_2} b.nf(\tau.b^1_b + \tau.b^2_b) \rfloor (nf(\tau.d^1_\sigma + \tau.d^2_\sigma)).$$

    Again $d'' \ll^c \tau.q_j$ and by induction $d'' \leq_E \tau.q_j$. By $\sigma\tau 2$ $d' \leq_E d''$ and so $d' \leq_E \tau.q_j$ as required.

  This completes the induction on $|I'|$ and hence we have shown $d' \leq_E \tau.q_j$.

We now need to show that $d' \leq_E d''$. Fortunately this follows directly from $\tau 4$.

That ends the final case in our partial completeness proof.

□

As an immediate corollary we have a completeness proof for arbitrary closed terms.

Theorem 4.16 *(Completeness)*
For arbitrary closed terms p, q, $p \sqsubseteq^c q$ implies $\vdash_E p \leq q$.

Proof: Suppose $p \ll^+ q$. In order to establish $\vdash_E p \leq q$, using $\omega - Induction$, it is sufficient to show $\vdash_E d \leq q$ for an arbitrary finite approximation d of p. But $p \ll^+ q$ implies $d \ll^+ q$ and therefore $\vdash_E d \leq q$ follows from the previous result. □

To finish this section let us now address the soundness of the system.

Theorem 4.17 *(Soundness)*

For arbitrary closed terms p, q, $\vdash_E p \leq q$ implies $p \sqsubseteq^c q$.

Proof: We have already shown that the inequations are sound and there are only two non-trivial rules:

1. The Stability Rule. For any set of closed processes $\{p_i : i \in I\}$ it is easy to check that $\sum_I \alpha_i.p_i \sim recx.\lfloor \sum_I \alpha_i.p_i \rfloor(x)$ from which the soundness follows.

2. ω-Induction. The proof of soundness of this rule is similar in spirit to that in [He88]. It is sufficient to establish that for any experiment e, p *must* e implies d *must* e for some finite approximation d of p. In [He88] it was sufficient to prove this for finite experiments e and induction was used on the size of e. Here we can not use this measure of induction since it may be possible that $e \xrightarrow{\sigma} e$. Instead we use another measure which does not depend on the fact that e is finite.

   Let us abbreviate the computation

   $$e|p = e_0|p_0 \mapsto e_1|p_1 \mapsto ...e_k|p_k$$

   to

   $$e|p \mapsto^n e_k|p_k$$

   if

   (a) for every $i \geq 0$ $\;e_i$ can not report success

   (b) in the derivation above the inferences

   $$e \xrightarrow{a} e',\ p \xrightarrow{\overline{a}} p' \text{ implies } e|p \mapsto e'|p'$$

   or

   $$e \xrightarrow{\sigma} e',\ p \xrightarrow{\sigma} p' \text{ implies } e|p \mapsto e'|p'$$

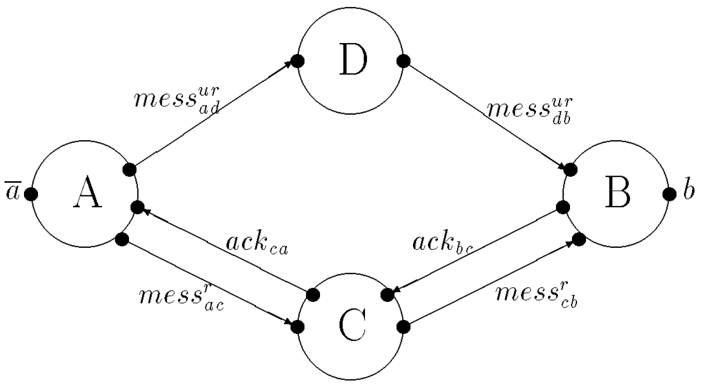
   are used n times.

   One can show that if p *must* e then the set $\{n \mid e|p \mapsto^n e'|p'\}$ is finite. One can now mimic the corresponding proof in [He88], Lemma 4.5.6, but using induction on the maximal element of this set.

□

5 Example

We present in this section a description of a very simple 'Security Costs Protocol'. The 'Security Costs Protocol' describes the transition of a message between two distributed ports. Transmission of a message across a secure medium is considered expensive while acknowledgements travel freely. The protocol initially sends the message across an unsecure medium only resending across the secure medium if an acknowledgement has not arrived before 'timeout'.



Accept:

$$A \Leftarrow \overline{a}.mess^{ur}_{ad}.(\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)$$

Reliable Medium:

$$C \Leftarrow \overline{mess^{r}_{ac}}.mess^{r}_{cb}.C + \overline{ack_{bc}}.ack_{ca}.C$$

Unreliable Medium:

$$D \Leftarrow \overline{mess^{ur}_{ad}}.(\tau.D + \tau.mess^{ur}_{db}.D)$$

Transmission:

$$B \Leftarrow \overline{mess^{ur}_{db}}.ack_{bc}.b.ack_{bc}.B + \overline{mess^{r}_{cb}}.b.ack_{bc}.B$$

$$System \Leftarrow (A|B|C|D) \setminus S \quad where \;\; S = Sort(A) \cup Sort(B) \cup Sort(C) \cup Sort(D) \setminus \{a, b\}$$

The message is received by the protocol on port $\overline{a}$. This is done at the module A, "Accept". A then sends the message to the unreliable medium, D, along port $mess^{ur}_{ad}$. D now either passes the message on to the final module of the protocol (B, "Transmission") along port $mess^{ur}_{db}$, or it losses the message. Upon the possible receipt of the message from D, B will send an acknowledgement to A via the reliable medium along ports ack_{bc} and ack_{ca}. If A does not receive this acknowledgement, then D has lost the message and after one time unit A will retransmit it to the reliable medium along port $mess^{r}_{ac}$. This is then passed onto B by the reliable medium, C, along port $mess^{r}_{cb}$. When the environment has accepted transmission of the message from B an acknowledgement is sent to A so that it can reset and be ready to receive another message. This final point avoids A receiving a second message before the delivery of the first. So in the summand $\overline{mess^{ur}_{db}}.ack_{bc}.b.ack_{bc}.B$ of B the first ack_{bc} represents the acknowledgement "message received over unreliable medium, do not resend" whilst the second ack_{bc} represents "message delivered to environment, reset to accept a new message".

We can now prove equationally that

$$System = \overline{a}.(\tau.\sigma.b.System + \tau.b.System)$$

$$\begin{array}{lll}
 & System = (A|B|C|D) \setminus S & by\ definition \\
= & \overline{a}.(mess^{ur}_{ad}.(\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|B|C|D) \setminus S & by\ d1 \\
= & \overline{a}.\tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|B|C|(\tau.D + \tau.mess^{ur}_{db}.D)) \setminus S & by\ d1 \\
= & \overline{a}.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|B|C|(\tau.D + \tau.mess^{ur}_{db}.D)) \setminus S & by\ d5 \\
= & \overline{a}.(X + Y) & by\ d4
\end{array}$$

$$w = \sum_A a.w_a,\ x = \sum_B b.x_b,\ y = \sum_C c.y_c,\ z = \sum_D d.z_d$$
$$\begin{array}{rcl}
(w|x|y|z) \setminus E & = & ext + int \\
\text{where} & & \\
ext & = & \sum_{A\setminus E} a.((w_a|x|y|z) \setminus E) + \sum_{B\setminus E} b.((w|x_b|y|z) \setminus E) + \\
 & & \sum_{C\setminus E} c.((w|x|y_c|z) \setminus E) + \sum_{D\setminus E} d.((w|x|y|z_d) \setminus E) \\
int & = & \sum_{A\cap\overline{B}} \tau.((w_a|x_b|y|z) \setminus E) + \sum_{A\cap\overline{C}} \tau.((w_a|x|y_c|z) \setminus E) + \\
 & & \sum_{A\cap\overline{D}} \tau.((w_a|x|y|z_d) \setminus E) + \sum_{B\cap\overline{C}} \tau.((w|x_b|y_c|z) \setminus E) + \\
 & & \sum_{B\cap\overline{D}} \tau.((w|x_b|y|z_d) \setminus E) + \sum_{C\cap\overline{D}} \tau.((w|x|y_c|z_d) \setminus E) \qquad d1
\end{array}$$

$$w = \sum_A a.w_a + \sigma.w_\sigma,\ x = \sum_B b.x_b,\ y = \sum_C c.y_c,\ z = \sum_D d.z_d$$
$$\begin{array}{rcl}
(w|x|y|z) \setminus E & = & \sigma.(((\sum_A a.w_a + w_\sigma)|x|y|z) \setminus E) \\
 & & \text{if } A \cap \overline{B} = \emptyset \wedge A \cap \overline{C} = \emptyset \wedge A \cap \overline{D} = \emptyset \wedge \\
 & & B \cap \overline{C} = \emptyset \wedge B \cap \overline{D} = \emptyset \wedge C \cap \overline{D} = \emptyset \\
 & & \text{and } A \cup B \cup C \cup D \subseteq E \qquad d2
\end{array}$$

$$w = \sum_A a.w_a + \sigma.w_\sigma,\ x = \sum_B b.x_b,\ y = \sum_C c.y_c,\ z = \sum_D d.z_d$$
$$\begin{array}{rcl}
(w|x|y|z) \setminus E & = & ext + int \\
\text{where} & & \\
ext & = & \sum_{A\setminus E} a.((w_a|x|y|z) \setminus E) + \sum_{B\setminus E} b.((w|x_b|y|z) \setminus E) + \\
 & & \sum_{C\setminus E} c.((w|x|y_c|z) \setminus E) + \sum_{D\setminus E} d.((w|x|y|z_d) \setminus E) \\
int & = & \sum_{A\cap\overline{B}} \tau.((w_a|x_b|y|z) \setminus E) + \sum_{A\cap\overline{C}} \tau.((w_a|x|y_c|z) \setminus E) + \\
 & & \sum_{A\cap\overline{D}} \tau.((w_a|x|y|z_d) \setminus E) + \sum_{B\cap\overline{C}} \tau.((w|x_b|y_c|z) \setminus E) + \\
 & & \sum_{B\cap\overline{D}} \tau.((w|x_b|y|z_d) \setminus E) + \sum_{C\cap\overline{D}} \tau.((w|x|y_c|z_d) \setminus E) \\
 & & \text{if } A \cap \overline{B} \neq \emptyset \vee A \cap \overline{C} \neq \emptyset \vee A \cap \overline{D} \neq \emptyset \vee \\
 & & B \cap \overline{C} \neq \emptyset \vee B \cap \overline{D} \neq \emptyset \vee C \cap \overline{D} \neq \emptyset \qquad d3
\end{array}$$

$$(\tau.x + \tau.y)|z = \tau.x|z + \tau.y|z \qquad d4$$

$$\alpha\tau.x = \alpha.x \qquad d5$$

$$\tau.\sigma.\tau.x = \tau.\sigma.x \qquad d6$$

Figure 7: Derived Equations

$$\begin{array}{rcl}
where\ X & = & \tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^r_{ac}.\overline{ack_{ca}}.A)|B|C|D) \setminus S \\
Y & = & \tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^r_{ac}.\overline{ack_{ca}}.A)|B|C|mess^{ur}_{db}.D) \setminus S
\end{array}$$

Now X

$$\begin{array}{lll}
= & \tau.\sigma.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + mess^{r}_{ac}.\overline{ack_{ca}}.A)|B|C|D) \setminus S & by\ d2 \\
= & \tau.\sigma.\tau.(\overline{ack_{ca}}.A|B|mess^{r}_{cb}.C|D) \setminus S & by\ d1 \\
= & \tau.\sigma.\tau.\tau.(\overline{ack_{ca}}.A|b.ack_{bc}.B|C|D) \setminus S & by\ d1 \\
= & \tau.\sigma.\tau.\tau.b.(\overline{ack_{ca}}.A|ack_{bc}.B|C|D) \setminus S & by\ d1 \\
= & \tau.\sigma.\tau.\tau.b.\tau.(\overline{ack_{ca}}.A|B|ack_{ca}.C|D) \setminus S & by\ d1 \\
= & \tau.\sigma.\tau.\tau.b.\tau.\tau.(A|B|C|D) \setminus S & by\ d1 \\
= & \tau.\sigma.b.System & by\ d5, d6
\end{array}$$

And Y

$$\begin{array}{lll}
= & \tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|B|C|mess^{ur}_{db}.D) \setminus S & by\ definition \\
= & \tau.\tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|ack_{bc}.b.ack_{bc}.B|C|D) \setminus S & by\ d3 \\
= & \tau.\tau.\tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|b.ack_{bc}.B|ack_{ca}.C|D) \setminus S & by\ d3 \\
= & \tau.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|b.ack_{bc}.B|ack_{ca}.C|D) \setminus S & by\ d5 \\
= & \tau.(U+V) & by\ d3
\end{array}$$

$$\begin{array}{rcl}
where\ U & = & b.((\overline{ack_{ca}}.\overline{ack_{ca}}.A + \sigma.mess^{r}_{ac}.\overline{ack_{ca}}.A)|ack_{bc}.B|ack_{ca}.C|D) \setminus S \\
V & = & \tau.(\overline{ack_{ca}}.A|b.ack_{bc}.B|C|D) \setminus S
\end{array}$$

Again U

$$\begin{array}{lll}
= & b.\tau.(\overline{ack_{ca}}.A|ack_{bc}.B|C|D) \setminus S & by\ d3 \\
= & b.\tau.\tau.(\overline{ack_{ca}}.A|B|ack_{ca}.C|D) \setminus S & by\ d1 \\
= & b.\tau.\tau.\tau.(A|B|C|D) \setminus S & by\ d1 \\
= & b.System & by\ d5
\end{array}$$

And V

$$\begin{array}{lll}
= & \tau.(\overline{ack_{ca}}.A|b.ack_{bc}.B|C|D) \setminus S & by\ definition \\
= & \tau.b.(\overline{ack_{ca}}.A|ack_{bc}.B|C|D) \setminus S & by\ d1 \\
= & \tau.b.\tau.(\overline{ack_{ca}}.A|B|ack_{ca}.C|D) \setminus S & by\ d1 \\
= & \tau.b.\tau.\tau.(A|B|C|D) \setminus S & by\ d1 \\
= & \tau.b.System & by\ a2
\end{array}$$

So finally:
$System$

$$\begin{array}{lll}
= & \overline{a}.(\tau.\sigma.b.System + \tau.(b.System + \tau.b.System)) & from\ above \\
= & \overline{a}.(\tau.\sigma.b.System + \tau.b.System) & by\ \tau 1, d5
\end{array}$$

Figure 7 shows the new equations used in this proof. All of these except $d4$ are derived equations in our proof system; their derivations are straightforward but tedious. Every closed instance of $d4$ can also be derived but the axiom itself cannot. Its use is inessential but we employ it to make the proof more readable. We leave the reader to check its soundness using the alternative characterisation.

6 Related Work

There is now an extensive literature on timed process algebras which can be classified from many different viewpoints. For a general discussion on the varieties of timed process algebras the reader is refered to [Je91] but from the purely syntactic level they can be viewed as extensions of the three main process algebras, *ACP, CSP* and *CCS*, each of which represent three somewhat different approaches. For example [BB89] presents a real-time extension of *ACP*, [Re88] contains an extension of *CSP* called *Timed CSP* while *CCS* is the starting point for [MT90a] where the process algebra *TCCS* is defined. Moreover the starting point determines to some extent the type of work reported in these papers. In [Re88] a denotational model for *Timed CSP* is presented, reflecting the fact that much of the work on *CSP* is based on a denotational approach to semantics. Similarly the concern of the *ACP* school of semantics with algebraic theories influences the approach taken in [BB89] while the operational viewpoint, which underlies much of the research on *CCS* is reflected in [MT90a]. However in subsequent work by researchers from these schools this distinction is much less clear. For example in [Gr89] an operational semantics is given to a real-time extension of *ACP* while in [Sch91] *Timed CSP* is considered from the operational point of view of testing.

It is perhaps more fruitful to classify the different approaches by their view of time and the way it is represented semantically. Here the *ACP* and *CSP* approaches, as expounded in [BB89, Re88] respectively, have much in common. They both take time to be real-valued and, at least semantically, associate time directly with actions, as indeed is the case with [QAF89]; Thus actions occur at some specific point in time. This approach is very different from ours as can be seen if we try to compare *TPL* with *Real-time ACP* and Timed CSP using the informal terminology of the introduction. Nevertheless these languages have been very influential. They are very expressive, have sound semantic theories either based on forms of bisimulation equivalence, [Mil89], or *Refusals*, [Hoa85] and have been seen to be useful in real-time applications.

The other major approach to representing time is to introduce special actions to represent the passage of time, which the current paper shares with [Gr89, MT90a, NRSV92] and [Yi90, Yi91] although the basis for all those proposals may be found in [BC84]. All of the languages presented in these papers share many of the underlying informal assumptions of *TPL* outlined in the introduction. For example they all continue to assume that actions are instantaneous and only the extension of *ACP* presented in [Gr89] does not incorporate *time determinism*; however *maximal progress* is less popular as an assumption and *patience* is even rarer. Although each of these proposals use a different syntax for their timed versions of process algebras it is of more interest to classify them according to the assumptions they impose on the special "time" actions.

In [Gr89], the simplest proposal, time is just like any other action except that it must synchronise across parallel bar. This fits in very neatly with the general synchronisation mechanism of *ACP* and an axiomatisation of weak bisimulation for finite terms in an extension of *ACP* with this timed action is given. In [MT90] a similar action is introduced into *CCS* but it assumes more of the characteristics of time; time determinism is assumed but they are uncommitted as to whether time is discrete or continuous. They give a complete axiomatisation of strong bisimulation for finite terms in a rather expressive language. The language, and operational semantics, in [NRSV92] is similar in spirit to *TPL* but is based on a different algebra *ACP*. In fact it is from this language that the

$\lfloor \_ \rfloor (\_)$ operator comes. Although they pay much attention to showing that their language is of use in describing realistic phenomena they also develop an equational theory for strong bisimulation. Neither of [NRSV92], [MT90] assume *maximal progress* but in its place they have *insistent* actions, i.e. actions which will not delay until the next time cycle. Needless to say the presence of insistent actions means that in general processes are not *patient*, in the informal terminology of the introduction. It seems that in timed process algebras in general either *maximal progress* is assumed or insistent actions are allowed; this is reasonable as both provide a mechanism for forcing actions to happen.

The language presented in [Yi90, Yi91] is the closest in spirit to our language; in fact it can in some sense be viewed as a real-time version of *TPL* as it assumes that actions are instantaneous in addition to *time determinism, maximal progress* and *patience*. However as with [Gr89, MT90a, NRSV92] its semantic theory is based on bisimulation theory. It is also somewhat more expressive than *TPL* in that, roughly speaking, it has prefix constructs of the form

$$a(t).P(t)$$

which represents a process which can perform the action a at any time t and then act like the process $P(t)$; so the behaviour of processes can in some sense be parameterised on the time when actions are performed.

Thus the approach we have taken has much in common with that of [Gr89, MT90a, NRSV92, Yi90, Yi91]. A major feature of this common approach is that the action representing time has special features which are incorporated into the operational semantics of the various languages using some form of prioritisation of the actions. Indeed it is shown in [Jef92] that many timed languages which take this approach can be translated into an untimed language where actions have associated with them a priority. However our semantic theory is based on testing and as far as we know the problem of developing a testing based semantic theory for timed processes has not been tackled before although, as we have previously mentioned a construct similar to σ has been used in [Ph87, La89] to describe so-called "refusal" tests. We have deliberately chosen a rather simple notion of time and in this choice we were very influenced by the preliminary exploration in [Ste88] carried out as part of the FORMAP project.

But now that a firm basis has been laid for a testing based theory we hope to be able to extend it to languages with more complicated constructs. The extension to the constructs of [Yi91] which are parameterised on time should be straightforward but to handle processes which are not *patient* will require a reworking of the notion of barb. Finally extending the theory of tests for a language where time is not discrete will be a major challenge.

References

[Ab90] Abramsky, S., "A Domain Equation for Bisimulation", Information and Control, vol 92, pp 161–218, 1991

[AH90] Arun-Kumar, S. and Hennessy, M., "An Efficiency Preorder for Processes", Acta Informatica, 29, pp 737-760, 1992.

[BB89] Baeten, J. and Bergstra, J., "Real Time Process Algebra", Formal Aspects of Computer Science, vol 3, pp 142–188, 1991.

[BW90a] Baeten, J. and Weijland, W., "Process Algebra", Cambridge University Press, 1990.

[BW90b] Baeten, J. and Weijland, W., "Applications of Process Algebra", Cambridge University Press, 1990.

[BC84] Berry, G. and Cosserat, L., "The ESTEREL Synchronous Programming Language and its Mathematical Semantics", Technical Report 842, INRIA, Sophia-Antipolis, 1988.

[BW89] Burns, A. and Wellings A., "Real-Time Systems and their Programming Languages", Adison-Wesley, 1989.

[CH88] Cleaveland, R. and Hennessy, M., "Priorities in Process Algebras", Information and Control, vol 87, nos 1/2, July/August, pp 58–77, 1990.

[CPW86] Cohen, B., Pitt, D.H. and Woodcock, J.C.P., "The Importance of Time in The Specification of OST Protocols", Technical Report, NPL, London, 1986.

[DS89] Davies, J. and Schneider, S., "An Introduction to Timed CSP", Technical Report, PRG, Oxford, 1989.

[dNH84] De Nicola, R. and Hennessy, M., "Testing Equivalence for Processes" *Theoretical Computer Science* vol.34, pp 83-133, North-Holland, 1984.

[GB87] Gert, R. and Boucher, A., "A timed failures model for extended communication processes", *Springer-Verlag Lecture Notes in Computer Science* vol.267, pp 95-114, 1986.

[vG88] van Glabbeek, R., "The Linear Time-Branching Time Spectrum", Proc. CONCUR90, Lecture Notes in Computer Science, vol 458, pp 278–297, Springer-Verlag, 1990.

[Gr89] Groote, J.F., "Specification and Verification of Real Time Systems in ACP" Technical Report CS-R9015, CWI, Amsterdam, 1989. An extended abstract appeared in L. Logrippo, R.L. Probert and H. Ural, editors, *Proceedings* 10^{th} *International Symposium on Protocol Specification, Testing and Verification*, Ottawa, pages 261–274, 1990.

[He88] Hennessy, M., "Algebraic Theory of Processes", MIT Press, Cambridge, 1988.

[He83] Hennessy, M., "Synchronous and Asynchronous Experiments on Processes", *Information and Control*, Vol 59, No 1-3, pp 36-83, 1983.

[He81] Hennessy, M., "A Term Model for Synchronous Processes", *Information and Control*, Vol 51, No 1, pp 58-75, 1981.

[HR90] Hennessy, M. and Regan, T., "A Temporal Process Algebra" University of Sussex Computer Science Technical Report 2:90, 1990.

[Hoa85] Hoare, C.A.R., "Communicating Sequential Processes", Prentice-Hall, 1985.

[HdR89] Hooman, J.J.M and deRoever, W.P. "Design and Verification in Real-Time Distributed Computing: an Introduction to Compositional Methods", Proceedings of the Ninth International Conference on Protocol Specification, Testing and Verification. North Holland, 1989.

[Je91] Jeffrey, A., "Discrete Timed CSP", Technical Report PMG 79, Chalmers University of Technology, Sweden, 1991.

[Je91a] Jeffrey, A., "Timed Process Algebra $\neq$ Time $\times$ Process Algebra" Technical Report PMG 78, Chalmers University of Technology, Sweden, 1991.

[Jef92] "Translating Timed Process Algebra into Untimed Process Algebra", Proc. Formal Techniques in Real-Time and Fault-Tolerant systems, *Springer-Verlag Lecture Notes in Computer Science* vol 571, 1992.

[Kn75] Knuth, D., "Fundamental Algorithms", Adison-Wesley, 1975.

[La89] Langerak, R., "A Testing Theory for LOTOS Using Deadlock Detection", Proceedings of the Ninth International Conference on Protocol Specification, Testing and Verification. North Holland, 1989.

[Mil83] Milner, R., "Calculi for Synchrony and Asynchrony", Theoretical Computer Science pp 267–310, 1983.

[Mil89] Milner, R., "Calculus for Communication and Concurrency", Prentice-Hall, London 1989.

[Mil90] Milner, R., "Operational and Algebraic Semantics of Concurrent Processes", Hanbook of Theoretical Computer Science, North-Holland, 1990.

[MT90] Moller, F. and Tofts, C., "A Temporal Calculus of Communicating Systems" Proceedings of CONCUR 90, Springer-Verlag Lecture Notes in Computer Science vol 458, pp 401–415, 1990.

[MT90a] Moller, F. and Tofts, C., "A Temporal Calculus of Communicating Systems" *Springer-Verlag Lecture Notes in Computer Science*, vol.458, pp 401-415, 1990.

[MT90b] Moller, F. and Tofts, C., "Relating Processes With Respect To Speed" Technical Report, LFCS, Edinburgh, 1991.

[Mur90] Murphy, D.V.J., "Time, Casuality, and Concurrency" PhD Thesis, University of Glasgow, CSC 90/R32, 1990.

[NRSV92] Nicollin, X., Richier, JL., Sifakis, J. and Voiron, J., "ATP: an Algebra for Timed Processes", to appear in Information and Control, 1992.

[Ph87] Phillips, I., "Refusal Testing", *Theoretical Computer Science*, vol.50, pp 241-284, 1987.

[Ph88] Phillips, I., "CCS With Broadcast Stability", Draft Technical Report, Imperial College, 1988.

[Pn85] Pneuli, A., "Linear and Branching Structures in the Semantics and Logics of Reactive Systems", *Springer-Verlag Lecture Notes in Computer Science* vol.194, pp 15-32, 1985.

[QAF89] Quemada, J., Azcorra, A. and Frutos, D., "TIC: A Timed Calculus for LOTOS", Technical Report, Madrid, 1989.

[Re88] Reed, G.M., "A Hierarchy of Domains for Real Time Distributed Computing" Technical Report, Oxford, 1988.

[Rea91] Regan, T., "Process Algebras for Real-Time Systems", PhD Thesis University of Sussex, 1991.

[RR86] Reed, G.M. and Roscoe, A., "A Timed model for communicating sequential processes", *Springer-Verlag Lecture Notes in Computer Science*, vol.226, pp 314-323, 1986.

[RS88] Rudkin, S. and Smith, C.R., "A Temporal Enhancement for LOTOS" British Telecom R and T ,1988.

[Sch86] Schmidt, D.A., "Denotational Semantics", Allyn and Bacon, 1986.

[Sch90] Schneider, S.A., "Correctness and Communication of Real-Time Systems", PhD Thesis, PRG, University of Oxford, 1990.

[Sch91] Schneider, S.A., "An Operational Semantics for Timed CSP", To appear in Information and Computation, 1992.

[Ste88] Steggles, P., "A Suggestion for a New Temporal LOTOS Semantics", Technical Report, GEC, 1988.

[Wi85] Winskel, G., "A Complete Proof System for SCCS With Modal Assertions" Technical Report, Cambridge, 1985.

[Yi90] Yi, W., "Real-Time Behavior of Asynchronous Agents", *Springer-Verlag Lecture Notes in Computer Science*, vol.458, pp 502-520, 1990.

[Yi91] Yi, W., " A Calculus of Real Time Systems", Ph.D Thesis, Chalmers University, 1991.

[Ze89] Zedan, H. (ed), "Real -Time Systems Theory and Applications", North-Holland, 1989.

[Jo89] Joseph, M., "Time and Real-time in Programs", *Springer-Verlag Lecture Notes in Computer Science* vol.405, FST & TCS 9, Bangalore, 1989.

[Ch91] Chen, L., "Decidability and Completeness in Real-Time Processes", Technical Report, LFCS, Edinburgh, 1991.

[Je91b] Jeffrey, A., "A Linear Time Process Algebra", CAV 91, 1991.

[MT91] Moller, F. and Tofts, C., “Relating Processes With Respect to Speed”, *Springer-Verlag Lecture Notes in Computer Science* vol.527, CONCUR 91, pp 424-438, 1991.

[Kl91] Klusener, A.S., “Completeness in Real Time Process Algebra”, *Springer-Verlag Lecture Notes in Computer Science* vol.527, CONCUR 91, pp 96-110, 1991.