On an inference rule for parallel Composition.

In this note we present a simple model of parallel processes which suffices to verify a proof rule of Cliff Jones for the parallel composition of processes.

For many purposes the meaning of a sequential process can be adequately represented by the set of those finite or infinite sequences of states

(*) $\sigma_0, \sigma_1, \cdots, \sigma_i, \sigma_{i+1} \cdots$

that the process allows. Here each transition step σ_i, σ_{i+1} is directly controlled by the process. When such processes act in parallel it is necessary to take into account that a transition step may not be directly controlled by the process but is the

result of interference from some other process. When ~~a sequence (*) is given~~ the transition steps σ_i, σ_{i+1} of a sequence (*) are classified into the two categories

(1) direct step
(2) interference step

then the result will be called an <u>action</u>.

The meaning of a process will be represented by the set of actions that the process allows. For example the process $x := 1$ might be represented by the set of those actions $\underline{\sigma}$ having state sequence (*) such that exactly one step σ_i, σ_{i+1} of $\underline{\sigma}$ is a direct step and then σ_{i+1} is obtained from σ_i by giving x the value 1.

The parallel composition $S_1 \| S_2$ of two processes S_1 and S_2 can now be explained in terms of the conjoining $\underline{\sigma}^1 \| \underline{\sigma}^2$ of compatible actions $\underline{\sigma}^1$ and $\underline{\sigma}^2$ allowed by S_1 and S_2 respectively.

$\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$ are <u>compatible</u> if

(1) they involve the same sequence of states.

(2) $\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$ have no direct steps in common.

For compatible $\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$ the <u>conjoining</u>, $\sigma_{\rightarrow}^1 \| \sigma_{\rightarrow}^2$, of $\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$ is defined to be that action, having the sequence of states that is common to both $\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$, where a direct step of the conjoined action is defined to be a step that is either a direct step of $\sigma_{\rightarrow}^1$ or a direct step of $\sigma_{\rightarrow}^2$.

$S_1 \| S_2$ is defined to be the process that allows all actions $\sigma_{\rightarrow}^1 \| \sigma_{\rightarrow}^2$ that are obtained by conjoining compatible actions $\sigma_{\rightarrow}^1$ and $\sigma_{\rightarrow}^2$ allowed by S_1 and S_2 respectively.

How should processes allowing interference be specified? Cliff Jones suggests that a specification <u>spec</u> should have the form

(pre P, rely R, guar G, post Q)

where P is a predicate of one state and R, G and Q are predicates of two states,

i.e. of steps σ_1, σ_2.

A process S satisfies such a specification (written S sat spec) if for every action $\xrightarrow{\sigma}$ allowed by S that starts in a state σ_0 satisfying P:

I. $\xrightarrow{\sigma}$ terminates in a state σ_n such that σ_0, σ_n satisfies Q, provided that every interference step of $\xrightarrow{\sigma}$ satisfies R.

II. Every direct step of $\xrightarrow{\sigma}$ satisfies G provided that all interference steps previous to the direct steps satisfy R.

Here is a formulation of Cliff Jones' inference rule:

The Inference rule for parallel composition.

FROM

Premise 1. S_1 sat (pre P, rely $R \vee G_2$, guar G_1, post Q_1)

Premise 2. S_2 sat (pre P, rely $R \vee G_1$, guar G_2, post Q_2)

INFER

Conclusion $S_1 || S_2$ sat (pre P, rely R, guar G, post Q)

PROVIDED THAT

SC1. $G_1 \vee G_2 \Rightarrow G$

SC2. $\overleftarrow{P} \wedge Q_1 \wedge Q_2 \wedge (R \vee G_1 \vee G_2)^* \Rightarrow Q$,

where $(\ )^*$ is the reflexive, transitive closure operation on predicates.

Soundness Proof.

Assume the premises and side conditions. Let $\underset{\rightarrow}{\sigma} = \underset{\rightarrow}{\sigma}^1 \| \underset{\rightarrow}{\sigma}^2$ where $\underset{\rightarrow}{\sigma}^1$ and $\underset{\rightarrow}{\sigma}^2$ are compatible actions allowed by S_1 and S_2 respectively, whose starting state σ_0 satisfies P.

Lemma. Let σ_i, σ_{i+1} be a direct step of $\underset{\rightarrow}{\sigma}$ whose previous interference steps satisfy R. Then the direct step satisfies G_1 if it is a direct step of $\underset{\rightarrow}{\sigma}^1$ and G_2 if it is a direct step of $\underset{\rightarrow}{\sigma}^2$.

Proof. This is by induction along the action $\underset{\rightarrow}{\sigma}$. So we assume the result for the previous direct steps of $\underset{\rightarrow}{\sigma}$. But every previous interference step of $\underset{\rightarrow}{\sigma}^1$ is either an interference step of $\underset{\rightarrow}{\sigma}$, when it satisfies R or else it is a direct step of $\underset{\rightarrow}{\sigma}^2$, in which case it satisfies G_2 by the induction hypothesis. In either case it satisfies $R \vee G_2$. Hence using II of promise I, if σ_i, σ_{i+1} is a direct step of $\underset{\rightarrow}{\sigma}^1$ then it must satisfy G_1. A similar argument (interchanging $\underset{\rightarrow}{\sigma}^1$ and $\underset{\rightarrow}{\sigma}^2$) shows that if σ_i, σ_{i+1} is a direct step of $\underset{\rightarrow}{\sigma}^2$ then it satisfies G_2.

Proof of I. Assume that every interference step of $\sigma_\Rightarrow$ satisfies R. By the lemma and its proof it follows that every interference step of $\sigma_\Rightarrow'$ must satisfy $R \vee G_2$ so that by premise 1 $\sigma_\Rightarrow'$ must terminate in a state σ_n such that σ_0, σ_n satisfies Q_1. Similarly, using premise 2 σ_0, σ_n must satisfy Q_2. As σ_0, σ_n trivially satisfies $\Leftarrow P$ it only remains to show that each step satisfies $R \vee G_1 \vee G_2$ as ~~[illegible]~~ then σ_0, σ_n will satisfy $(R \vee G_1 \vee G_2)^*$ and we may then apply SC2 to deduce that it also satisfies Q. Each step of $\sigma_\Rightarrow$ must either be an interference step of $\sigma_\Rightarrow'$ or of $\sigma_\Rightarrow^2$. Hence by the above it must either satisfy $R \vee G_1$ or $R \vee G_2$. In either case it does satisfy $R \vee G_1 \vee G_2$.

Proof of II. Assume given a direct step of $\sigma_\Rightarrow$ whose previous interfering steps satisfy R. Then by the lemma the direct step must satisfy $G_1 \vee G_2$ and hence G using SC1.