◇ Traces ◇

A *trace* of a process is a finite sequence of events, representing the behaviour of the process up to a certain point in time. Traces are written as comma-separated sequences of events, enclosed in angle brackets: for example, $\langle coin, choc, coin \rangle$. This is a trace of the recursive version of VM.

Example: $\langle open, close \rangle$ and $\langle open, close, open \rangle$ are traces of $DOOR$.

$(DOOR = open \rightarrow close \rightarrow DOOR)$

Example: $\langle staines, pound \rangle$ and $\langle ashford, pound \rangle$ are traces of $TICKET$, and also of $TICKETS$.

We will only consider *finite* traces.

The empty trace, containing no events, is written $\langle \rangle$ and pronounced "empty" or "nil". It is a trace of every process, corresponding to an observation when no event has yet happened.

If a process is defined without recursion, then it only has a finite set of traces. For example, if

$$PHONE = ring \rightarrow answer \rightarrow Stop$$

then the only traces of $PHONE$ are $\langle \rangle$, $\langle ring \rangle$ and $\langle ring, answer \rangle$.

A recursive process, which can keep performing events forever, has an infinite set of traces. For example, if

$$\mathit{CLOCK} = \mathit{tick} \rightarrow \mathit{CLOCK}$$

then the traces of CLOCK are

$$\langle\rangle, \langle \mathit{tick}\rangle, \langle \mathit{tick}, \mathit{tick}\rangle, \langle \mathit{tick}, \mathit{tick}, \mathit{tick}\rangle, \ldots$$

It is important to be clear about the fact that we are interested in potentially *infinite* sets of *finite* traces.

◇ Operations on Traces ◇

We will use various operations on traces, and a number of facts or laws about them. Most of the laws are rather obvious.

◇ Concatenation ◇

The first operation is *concatenation*, also called *catenation*. It joins traces together into longer traces:

$$\langle a_1, \ldots, a_m\rangle \frown \langle b_1, \ldots, b_n\rangle = \langle a_1, \ldots, a_m, b_1, \ldots, b_n\rangle.$$

Example: $\langle \mathit{coin}, \mathit{choc}\rangle \frown \langle \mathit{choc}\rangle = \langle \mathit{coin}, \mathit{choc}, \mathit{choc}\rangle$.

Concatenation is associative, and the empty trace is a unit, i.e.

$$s \frown (t \frown u) = (s \frown t) \frown u$$
$$\langle\rangle \frown s = s = s \frown \langle\rangle$$

The following laws are useful:

$$s \frown t = s \frown u \text{ if and only if } t = u$$
$$s \frown u = t \frown u \text{ if and only if } s = t$$
$$s \frown t = \langle\rangle \text{ if and only if } s = \langle\rangle \text{ and } t = \langle\rangle$$

If n is a positive integer, then t^n is defined to be n copies of the trace t concatenated together. t^n can be defined recursively by

$$\begin{aligned} t^0 &= \langle\rangle \\ t^{n+1} &= t \frown t^n. \end{aligned}$$

◇ Functions on Traces ◇

Suppose f is a function which maps traces to traces. f is said to be *strict* if $f(\langle\rangle) = \langle\rangle$, and *distributive* if $f(s \frown t) = f(s) \frown f(t)$.

In fact, any distributive function is strict: if f is distributive then

$$\begin{aligned} f(s) \frown \langle\rangle &= f(s) \\ &= f(s \frown \langle\rangle) \\ &= f(s) \frown f(\langle\rangle) \end{aligned}$$

and so $f(\langle\rangle) = \langle\rangle$.

If f is distributive then its action on traces can be put together from its action on single-event traces:

$$\begin{aligned} f(\langle a_1, \ldots, a_n\rangle) &= f(\langle a_1\rangle \frown \ldots \frown \langle a_n\rangle) \\ &= f(\langle a_1\rangle) \frown \ldots \frown f(\langle a_n\rangle). \end{aligned}$$

$\diamond$ Restriction $\diamond$

The expression $t \restriction A$ denotes the trace t when *restricted* to events in the set A. $t \restriction A$ consists of t with all events outside A omitted.

Example: $\langle \mathit{start}, \mathit{exercise}, \mathit{exercise}, \mathit{end} \rangle \restriction \{\mathit{start}, \mathit{end}\} = \langle \mathit{start}, \mathit{end} \rangle$.

$\langle \mathit{start}, \mathit{exercise}, \mathit{exercise}, \mathit{end} \rangle \restriction \{\mathit{start}, \mathit{exercise}\} = \langle \mathit{start}, \mathit{exercise}, \mathit{exercise} \rangle$.

Restriction is distributive and therefore strict:

$$\begin{aligned} \langle\rangle \restriction A &= \langle\rangle \\ (s \frown t) \restriction A &= (s \restriction A) \frown (t \restriction A). \end{aligned}$$

The effect of restriction on single-event traces is clear:

$$\begin{aligned} \langle x \rangle \restriction A &= \langle x \rangle \text{ if } x \in A \\ \langle x \rangle \restriction A &= \langle\rangle \text{ if } x \notin A \end{aligned}$$

Two other facts:

$$\begin{aligned} s \restriction \{\} &= \langle\rangle \\ (s \restriction A) \restriction B &= s \restriction (A \cap B) \end{aligned}$$

$\diamond$ Head and Tail $\diamond$

If s is a non-empty trace, its first event is denoted s_0 and the trace consisting of all events after the first is denoted s'.

Neither $\langle\rangle_0$ nor $\langle\rangle'$ is defined.

Example: $\langle \mathit{coin}, \mathit{choc}\rangle_0 = \mathit{coin}$.

$\langle \mathit{coin}, \mathit{choc}\rangle' = \langle \mathit{choc}\rangle$.

A few facts:

$$\begin{aligned} (\langle x\rangle \frown s)_0 &= x \\ (\langle x\rangle \frown s)' &= s \\ s &= \langle s_0\rangle \frown s' \end{aligned}$$

$\diamond$ Star $\diamond$

If A is a set of events, the set A^* is the set of all finite traces, including $\langle\rangle$, containing events from A.

Example:

$\{a, b\}^* = \{\langle\rangle, \langle a\rangle, \langle b\rangle, \langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle, \ldots\}$

$\diamond$ Ordering $\diamond$

A trace s is a *prefix* of a trace t if there is some extension u of s such that $s \frown u = t$. We then write $s \leqslant t$.

Example:

$$\begin{aligned} \langle a, b, c\rangle &\leqslant \langle a, b, c, d\rangle \\ \langle\rangle &\leqslant \langle a, b\rangle \end{aligned}$$

$\diamond$ Length $\diamond$

The length of the trace t is denoted $\#t$.

Example: $\#\langle a, b\rangle = 2$, $\#\langle\rangle = 0$.

$\diamond$ Traces of a Process $\diamond$

In general a process has many different possible behaviours, and we do not know in advance which traces will be generated by a particular execution. However, we can determine in advance the set of all possible traces of a process P. This set is written $traces(P)$.

Examples: $traces(Stop) = \{\langle\rangle\}$.

$traces(\mathsf{coin} \rightarrow Stop) = \{\langle\rangle, \langle \mathsf{coin}\rangle\}$.

$$\begin{aligned} traces(\mathsf{CLOCK}) &= \{\langle\rangle, \langle \mathsf{tick}\rangle, \langle \mathsf{tick}, \mathsf{tick}\rangle, \ldots\} \\ &= \{\mathsf{tick}\}^* \end{aligned}$$

We can now systematically write down definitions of $traces(P)$ for processes P constructed from the operators we have seen so far. We already know the definition for $Stop$:

$$traces(Stop) = \{\langle\rangle\}.$$

$traces(a \to P)$ is constructed from $traces(P)$ by the addition of a as an initial event:

$$traces(a \to P) = \{\langle\rangle\} \cup \{\langle a\rangle \frown t \mid t \in traces(P)\}.$$

Notice the addition of the trace $\langle\rangle$, which must always be a trace of any process.

The definition of $traces(a \to P \mid b \to Q)$ is similar, taking account of the two possible first events:

$$\begin{aligned} traces(a \to P \mid b \to Q) &= \{\langle\rangle\} \\ &\cup \{\langle a\rangle \frown t \mid t \in traces(P)\} \\ &\cup \{\langle b\rangle \frown t \mid t \in traces(Q)\}. \end{aligned}$$

Also similarly, we can give a general definition of $traces(x : A \to P(x))$.

$$\begin{aligned} & traces(x : A \to P(x)) \\ &\quad = \{\langle\rangle\} \\ &\quad \cup \{\langle a\rangle \frown t \mid a \in A, t \in traces(P(a))\}. \end{aligned}$$

A few facts about $traces$:

$\langle\rangle \in traces(P)$, for any P.

If $s \frown t \in traces(P)$ then $s \in traces(P)$.

$traces(P) \subseteq (\alpha P)^*$.

Describing the set of traces of a recursive process is more complicated. Suppose we have the definition

$$X = F(X)$$

where $F(X)$ is a guarded expression. Guardedness means that we know at least the possible first events of $F(X)$. In fact, they are the same as the possible first events of $F(Stop)$.

Example: If $X = a \to X$ then we know that X can do a first, and this is the same first event as in $a \to Stop$.

Depending on the form of $F(X)$, we may know more than just the first event.

Example: If $X = a \to b \to X \mid c \to X$ we know that X can either do a then b, or c, so we know that $\langle a, b\rangle$ and $\langle c\rangle$ are traces of X. They are also traces of $a \to b \to Stop \mid c \to Stop$.

We can discover some traces of X by looking at $F(Stop)$. For the traces corresponding to running through F twice, we need to look at $F(F(Stop))$.

Example: If $X = a \to X$ we also have

$$X = a \to a \to X$$

so $\langle a, a \rangle$ is a trace of X.

If $X = a \to b \to X \mid c \to X$ we also have

$$\begin{aligned} X \;=\; & a \to b \to (a \to b \to X \mid c \to X) \\ & \mid c \to (a \to b \to X \mid c \to X) \end{aligned}$$

So $\langle a, b, a \rangle$, $\langle a, b, c \rangle$, $\langle c, a, b \rangle$ etc. are traces of X.

In general we can define iteration of F:

$$\begin{aligned} F^0(X) &= X \\ F^{n+1}(X) &= F(F^n(X)) \end{aligned}$$

and then, for $X = F(X)$, we have

$$\begin{aligned} \mathit{traces}(X) &= \bigcup_{n \geqslant 0} \mathit{traces}(F^n(\mathit{Stop})) \\ &= \mathit{traces}(\mathit{Stop}) \cup \mathit{traces}(F(\mathit{Stop})) \\ &\cup\; \mathit{traces}(F(F(\mathit{Stop}))) \cup \ldots \end{aligned}$$

Of course, all this only makes sense if $F(X)$ is guarded.

Writing down the set of traces of a recursive process in a compact form is a little challenging. For example, if $X = a \to b \to X$, then $\mathit{traces}(X)$ contains not only $\langle a, b \rangle$, $\langle a, b, a, b \rangle$, $\langle a, b \rangle^3$ and so on, but also the intermediate traces ending in a. One way to describe $\mathit{traces}(X)$ is:

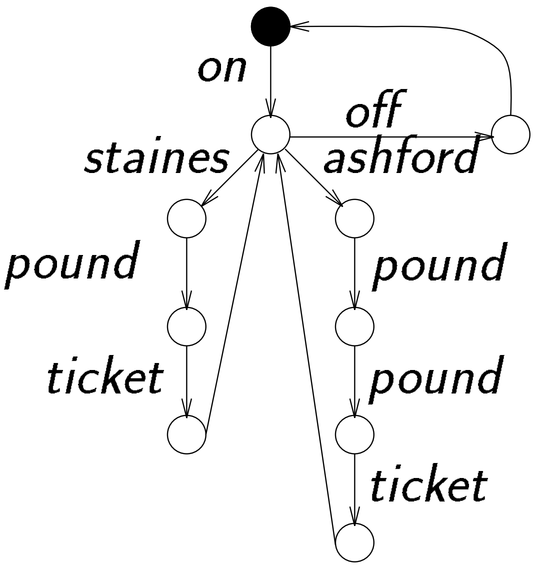
$$\mathit{traces}(X) = \{t \mid \text{for some } n,\ t \leqslant \langle a, b \rangle^n\}$$

◇ Traces and Diagrams ◇

There is a connection between the transition diagram of a process, and its traces. For example, recall the process *TICKETS* defined by

$$
\begin{aligned}
\mathit{MACHINE} &= \mathit{on} \rightarrow \mathit{TICKETS} \\
\mathit{TICKETS} &= \mathit{staines} \rightarrow \mathit{pound} \rightarrow \mathit{ticket} \rightarrow \mathit{TICKETS} \\
&\mid \mathit{ashford} \rightarrow \mathit{pound} \rightarrow \mathit{1pound} \rightarrow \mathit{ticket} \rightarrow \mathit{TICKETS} \\
&\mid \mathit{off} \rightarrow \mathit{MACHINE}
\end{aligned}
$$

and its transition diagram:



For any path through the diagram, starting from the black state, there is a trace consisting of the sequence of labels on the path. $traces(\mathit{TICKETS})$ is the set of traces corresponding to all these paths, including $\langle\rangle$ which corresponds to the empty path (i.e. simply remaining at the starting point).

◇ Traces and Transitions ◇

The operational semantics of CSP allows us to unwind the behaviour of a process, one event at a time. Looking at the traces of a process gives us an overall view. Since the traces can be extracted from a transition diagram, and labelled transitions are supposed to capture the same information as the diagrams, we should also be able to write down a relationship between a process' traces and its labelled transitions. Here it is:

$$traces(P) = \{\langle\rangle\} \\ \cup\ \{\langle a\rangle \frown t \mid P \xrightarrow{a} Q, t \in traces(Q)\}.$$

Later we will be defining new CSP operators, by means of labelled transition rules. We will use this relationship between transitions and traces to calculate the traces of processes defined in terms of the new operators.

◇ Exercises ◇

△ Write down $traces(\mathit{TICKET})$, where TICKET is defined as before by

$$\mathit{TICKET} = \mathit{staines} \to \mathit{pound} \to \mathit{ticket} \to Stop \\ \mid \mathit{ashford} \to \mathit{pound} \to \mathit{pound} \to \mathit{ticket} \to Stop$$

◇ Exercises ◇

- Define a process P such that
$$traces(P) = \{\langle\rangle, \langle a\rangle, \langle b\rangle, \langle b, c\rangle\}.$$

- Define a process P such that $\langle a, b, c\rangle$ and $\langle a, b, a\rangle$ are both traces of P.

- Is there a process P such that
$$traces(P) = \{\langle\rangle, \langle a\rangle, \langle a, b\rangle, \langle c, d\rangle\}?$$

$\diamond$ Traces for Concurrency $\diamond$

$$\begin{aligned} traces(P\ {}_A\|_B\ Q) \ = \ \{t \mid\ & t \in (A \cup B)^* \\ & \text{and } t \restriction A \in traces(P) \\ & \text{and } t \restriction B \in traces(Q)\} \end{aligned}$$

If $A = B$, this definition reduces to

$$\begin{aligned} traces(P\ {}_A\|_A\ Q) \ = \ \{t \mid\ & t \in A^* \\ & \text{and } t \restriction A \in traces(P) \\ & \text{and } t \restriction A \in traces(Q)\} \end{aligned}$$

i.e. $traces(P\ {}_A\|_A\ Q) = traces(P) \cap traces(Q)$, because if $t \in A^*$ then $t \restriction A = t$. This fits in with the earlier discussion of concurrency with the same alphabet.

If $A \cap B = \{\}$ then every event in a possible trace of $P\ {}_A\|_B\ Q$ is either an event from A or an event from B. In a trace t of $P\ {}_A\|_B\ Q$, the events from A (i.e. $t \restriction A$) must form a trace of P, and similarly the events from B must form a trace of Q. Any pair of traces, one from P and one from Q, can be *interleaved* to form a trace of $P\ {}_A\|_B\ Q$.

Example: $\langle \mathit{left}, \mathit{right}, \mathit{right} \rangle$ is a trace of *LR* and $\langle \mathit{up}, \mathit{down} \rangle$ is a trace of *UD*. So

$$\langle \mathit{left}, \mathit{up}, \mathit{down}, \mathit{right}, \mathit{right} \rangle$$

is a trace of *LR* $\|$ *UD*.

In general, a trace of P and a trace of Q can be used to form a trace of $P\ {}_A\|_B\ Q$ as long as the events in $A \cap B$ appear in the same order in both traces.

Example: $\langle \mathit{coin}, \mathit{beep}, \mathit{choc} \rangle$ is a trace of *VM* and $\langle \mathit{coin}, \mathit{shout}, \mathit{choc} \rangle$ is a trace of *CUST*. The events common to both alphabets (i.e. *coin* and *choc*) appear in the same order in both traces.

$\langle \mathit{coin}, \mathit{beep}, \mathit{shout}, \mathit{choc} \rangle$ and $\langle \mathit{coin}, \mathit{shout}, \mathit{beep}, \mathit{choc} \rangle$ are both traces of $\mathit{VM} \parallel \mathit{CUST}$.

$\diamond$ Trace Equivalence $\diamond$

We have spoken vaguely of processes being equivalent to each other — for example, a process which can do no events is equivalent to $Stop$. In CSP there are in fact several notions of process equivalence, each of which is useful in different situations. The first is *trace equivalence*, denoted by $=_t$, and defined by

$$P =_t Q$$
if and only if
$$traces(P) = traces(Q)$$

Two processes are trace equivalent if they have the same observable behaviour, as measured by $traces$.

Example: Consider the process

$$a \to Stop\ {}_{\{a,b\}}\|_{\{a,b\}}\ b \to Stop.$$

The definition of $traces$ for a parallel combination of processes gives
$traces(a \to Stop\ {}_{\{a,b\}}\|_{\{a,b\}}\ b \to Stop)$
$= \{t \in \{a, b\}^* \mid t\restriction\{a, b\} \in traces(a \to Stop)$
and $t\restriction\{a, b\} \in traces(b \to Stop)\}$.

i.e. $traces(a \to Stop\ {}_{\{a,b\}}\|_{\{a,b\}}\ b \to Stop)$
$= traces(a \to Stop) \cap traces(b \to Stop)$.

Because

$$traces(a \to Stop) = \{\langle\rangle, \langle a\rangle\}$$

and

$$traces(b \to Stop) = \{\langle\rangle, \langle b\rangle\}$$

we get

$$traces(a \to Stop\ {}_{\{a,b\}}\|_{\{a,b\}}\ b \to Stop) = \{\langle\rangle\}.$$

Therefore

$$a \to Stop\ {}_{\{a,b\}}\|_{\{a,b\}}\ b \to Stop =_t Stop.$$

◇ Refinement and Specification ◇

The *refinement* relation $\sqsubseteq_t$ on processes is defined by

$$P \sqsubseteq_t Q$$
if and only if
$$traces(Q) \subseteq traces(P)$$

$P \sqsubseteq_t Q$ is pronounced "P is refined by Q". The subscript t indicates that we are working with traces — later we will see other forms of refinement.

P is refined by Q if Q exhibits at most the behaviour exhibited by P — possibly less.

Example:

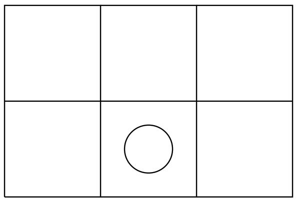
$$a \to b \to Stop \sqsubseteq_t a \to Stop$$

Example: For any process P, $P \sqsubseteq_t Stop$.

The main use of refinement is in specification. If we think of P as defining a range of permissible behaviour, then the statement $P \sqsubseteq_t Q$ can be read as the specification that Q's behaviour must stay within this range.

◇ Example ◇

Recall the example of a counter moving on a board.



$$
\begin{aligned}
\mathit{LR} &= \mathit{left} \rightarrow \mathit{right} \rightarrow \mathit{LR} \,\Box\, \mathit{right} \rightarrow \mathit{left} \rightarrow \mathit{LR} \\
\mathit{UD} &= \mathit{up} \rightarrow \mathit{down} \rightarrow \mathit{UD}
\end{aligned}
$$

$$\mathit{SPEC} = \mathit{LR} \;{}_{\{\mathit{left},\mathit{right}\}}\|_{\{\mathit{up},\mathit{down}\}}\; \mathit{UD}$$

We can now interpret SPEC as a specification for processes which might descibe movements of the counter. Because SPEC describes exactly the behaviours which correspond to staying on the board, the specification

$$\mathit{SPEC} \sqsubseteq_t P$$

specifies that P must describe movement within the board — possibly restricted movement.

For example,

$$\mathit{SPEC} \sqsubseteq_t \mathit{left} \rightarrow \mathit{up} \rightarrow \mathit{Stop}$$

which we can check by writing down all the traces of the process on the right and showing that they are all traces of SPEC.

The specification

$$\textit{SPEC} \sqsubseteq_t P$$

limits what P can do, but does not require it to do anything. For example,

$$\textit{SPEC} \sqsubseteq_t \mathit{Stop}.$$

Specifications which simply restrict behaviour without requiring any particular behaviour are known as *safety specifications*. They specify that nothing bad can happen, without specifying that anything good must happen. Stop satisfies any safety specification — doing nothing is always safe.

All specifications which can be expressed using trace refinement are safety specifications.

Specifications which require something positive to happen are called *liveness specifications*. We will see later how they can be expressed in CSP.

Example: If we define P by

$$P = \textit{left} \to \textit{left} \to \mathit{Stop}$$

then we do not have $\textit{SPEC} \sqsubseteq_t P$ because

$$\begin{array}{l}\langle \textit{left}, \textit{left} \rangle \ \in \ \mathit{traces}(P) \\ \langle \textit{left}, \textit{left} \rangle \ \notin \ \mathit{traces}(\textit{SPEC}).\end{array}$$

◇ The Level Crossing ◇

As an example of writing a specification in CSP, we will look at a railway level crossing. One road and one railway line cross each other, and as usual there is a gate which can be lowered to prevent cars crossing the railway. If the gate is raised, then cars can freely cross the track. Trains can cross the road regardless of whether the gate is up or down.

We will consider the obvious safety property for the level crossing, which is:

There should never be a train and a car on the crossing at the same time.

Of course there are many other properties which we might like to specify, for example a liveness property:

Whenever a car approaches the crossing, it should eventually be able to cross.

but for the moment we will stick to safety.

We will use the following events to represent the interesting aspects of the behaviour of the system.

car.approach, *car.enter*, *car.leave*, *train.approach*, *train.enter*, *train.leave*, *gate.lower*, *gate.raise*

The processes *CARS* and *TRAINS* supply streams of cars and trains.

$$\begin{aligned} \mathit{CARS} &= \mathit{car.approach} \to \mathit{car.enter} \to \\ &\quad\; \mathit{car.leave} \to \mathit{CARS} \\ \mathit{TRAINS} &= \mathit{train.approach} \to \mathit{train.enter} \to \\ &\quad\; \mathit{train.leave} \to \mathit{TRAINS} \end{aligned}$$

The following processes model the behaviour of the crossing. This is a complete description of all possibilities, including a car and a train simultaneously using the crossing. Later we will add a control process which uses the gate to restrict access by cars.

CR_UP and *CR_DOWN* model the crossing with the gate up and down, respectively. C, T, *CT* model the crossing when there is a car, train or both present.

$$\begin{aligned} \mathit{CR\_UP} &= \mathit{car.approach} \to \mathit{car.enter} \to C \\ &\;\;\square\;\; \mathit{train.approach} \to \mathit{train.enter} \to T \\ &\;\;\square\;\; \mathit{gate.down} \to \mathit{CR\_DOWN} \end{aligned}$$

$$\begin{aligned} C &= \mathit{car.leave} \to \mathit{CR\_UP} \\ &\;\;\square\;\; \mathit{train.approach} \to \mathit{train.enter} \to \mathit{CT} \\ T &= \mathit{train.leave} \to \mathit{CR\_UP} \\ &\;\;\square\;\; \mathit{car.approach} \to \mathit{car.enter} \to \mathit{CT} \end{aligned}$$

$$\mathit{CT} = \mathit{crash} \to \mathit{Stop}$$

$$\begin{aligned} \mathit{CR\_DOWN} \;=\;& \mathit{train.approach} \rightarrow \mathit{train.enter} \rightarrow \\ & \mathit{train.leave} \rightarrow \mathit{CR\_DOWN} \\ \square\;& \mathit{gate.up} \rightarrow \mathit{CR\_UP} \end{aligned}$$

Defining some sets of events:

$$\begin{aligned} E_T &= \{\mathit{train.approach}, \mathit{train.enter}, \mathit{train.leave}\} \\ E_C &= \{\mathit{car.approach}, \mathit{car.enter}, \mathit{car.leave}\} \\ E_G &= \{\mathit{gate.raise}, \mathit{gate.lower}\} \\ E_X &= \{\mathit{crash}\} \\ E_S &= E_T \cup E_C \cup E_G \cup E_X \end{aligned}$$

allows us to define the whole system as

$\mathit{SYSTEM} = (\mathit{CR\_UP}\ {}_{E_S}\|_{E_C}\ \mathit{CARS})\ {}_{E_S}\|_{E_T}\ \mathit{TRAINS}.$

To specify that no crashes occur, we need a process *SPEC* which can do any events except for *crash*.

$$\begin{aligned} \mathit{SPEC} \;=\;& \mathit{train}?x : \{\mathit{approach}, \mathit{enter}, \mathit{leave}\} \rightarrow \mathit{SPEC} \\ \square\;& \mathit{car}?x : \{\mathit{approach}, \mathit{enter}, \mathit{leave}\} \rightarrow \mathit{SPEC} \\ \square\;& \mathit{gate}?x : \{\mathit{raise}, \mathit{lower}\} \rightarrow \mathit{SPEC} \end{aligned}$$

In general, Run_A is the process which can repeatedly do events from the set A:

$$\mathit{Run}_A \;=\; x : A \rightarrow Run_A$$

so $\mathit{SPEC} = \mathit{Run}_{E_T \cup E_C \cup E_G}$.

The requirement that the crossing satisfies this specification is expressed by

$$\mathit{SPEC} \sqsubseteq_t \mathit{SYSTEM}.$$

It is possible to use the FDR tool to check trace refinement, and this is the easiest way to show that the specification is not satisfied (not surprisingly, as we haven't imposed any restrictions on when the gate can be raised or lowered).

Now we will define a process *CONTROL* which, when placed in parallel with *SYSTEM*, will constrain the behaviour so that whenever a train approaches the gate must be lowered. This will be achieved by making *CONTROL* and *SYSTEM* synchronise on certain events. We hope that the result will be a system which satisfies the safety specification.

$$\begin{array}{rcl} \mathit{CONTROL} & = & \mathit{train.approach} \rightarrow \mathit{gate.down} \rightarrow \\ & & \mathit{CONTROL\_D} \\ & \square & \mathit{car.approach} \rightarrow \mathit{car.enter} \rightarrow \\ & & \mathit{car.leave} \rightarrow \mathit{CONTROL} \\ \mathit{CONTROL\_D} & = & \mathit{train.enter} \rightarrow \mathit{train.leave} \rightarrow \\ & (& \mathit{train.approach} \rightarrow \mathit{CONTROL\_D} \\ & \square & \mathit{gate.up} \rightarrow \mathit{CONTROL}) \\ \mathit{SAFE\_SYSTEM} & = & \mathit{SYSTEM} \;{}_{E_S}\|_{E_T \cup E_C \cup E_G}\; \mathit{CONTROL} \end{array}$$

Again, FDR can be used to test whether

$$\mathit{SPEC} \sqsubseteq_t \mathit{SAFE\_SYSTEM}$$

and this time we will find that it does.

Here is an alternative way of checking *SYSTEM*. Notice that when a car and a train use the crossing at the same time, the event *crash* occurs, and the system stops. This is the only point at which we have deliberately introduced $Stop$ into the system, and we hope that there are no other deadlocks.

If we use FDR to check *SYSTEM* for deadlock-freedom, then every time a deadlock is found we will see a trace leading to $Stop$. If the trace ends in *crash*, then we have identified a violation of safety. If the trace ends with some other event, then there is another deadlock in the system, which presumably represents a mistake in our model.

In general there are many different ways of modelling a system, and many different ways of writing a specification. The challenge is to model the system in such a way that the bad property appears as a kind of behaviour (in this example, occurrence of *crash*) which can be ruled out by a suitable specification.

◇ Another Level Crossing ◇

Here is another way of modelling the level crossing. Remove the *crash* event, and change the definition of *CT* to

$$\begin{aligned} \mathit{CT} &= \mathit{car.leave} \rightarrow T \\ &\;\square\; \mathit{train.leave} \rightarrow C\,. \end{aligned}$$

Also change the definition of E_S to

$$E_S = E_C \cup E_T \cup E_G\,.$$

As before,

$$\mathit{SYSTEM} = (\mathit{CR\_UP}\ {}_{E_S}\|_{E_C}\ \mathit{CARS})\ {}_{E_S}\|_{E_T}\ \mathit{TRAINS}\,.$$

The specification now consists of two parts.

$$\begin{aligned} \mathit{SPEC1} &= \mathit{Run}_{E_G} \\ \mathit{SPEC2} &= \mathit{train.approach} \rightarrow \mathit{train.enter} \rightarrow \\ & \mathit{train.leave} \rightarrow \mathit{SPEC2} \\ &\;\square\; \mathit{car.approach} \rightarrow \mathit{car.enter} \rightarrow \\ & \mathit{car.leave} \rightarrow \mathit{SPEC2} \\ \mathit{SPEC} &= \mathit{SPEC1}\ {}_{E_G}\|_{E_T \cup E_C}\ \mathit{SPEC2} \end{aligned}$$

SPEC1 allows the gate to be raised and lowered freely. *SPEC2* only allows trains and cars to enter the crossing separately.

Again we can check

$$\mathit{SPEC} \sqsubseteq_t \mathit{SYSTEM}$$

which is not true, and define

$$\mathit{SAFE\_SYSTEM} = \mathit{SYSTEM} \ {}_{E_S}\|_{E_S} \ \mathit{CONTROL}$$

and check

$$\mathit{SPEC} \sqsubseteq_t \mathit{SAFE\_SYSTEM}$$

which is true.