Temporal Specification

[Refinement and Concurrency]

Michael Fisher

Department of Computer Science, University of Liverpool, UK

[MFisher@liverpool.ac.uk]
Imagine we have a temporal specification, $Spec$, about which we can establish some properties:

$$\vdash Spec \Rightarrow Properties$$

Now, maybe the specification we have lacks some details, so we produce a revised specification, say $Spec'$. Clearly we do not want to prove $\vdash Spec' \Rightarrow Properties$ if we can avoid it, and surely we would like all the behaviours of $Spec'$ to also be behaviours of $Spec$.

Thus, as in many formal specification techniques, we can refine $Spec$ to a new specification $Spec'$ as long as we can establish that

$$\vdash Spec' \Rightarrow Spec$$
Example

Let us consider a sample initial temporal specification and its refinement:

\[ Spec = p \land \Diamond q \]
\[ Spec' = p \land \Box q \]

Since \( \vdash (p \land \Box q) \Rightarrow (p \land \Diamond q) \), then \( Spec' \) is indeed a refinement of \( Spec \). Consequently, if we know that

\[ \vdash Spec \Rightarrow (\Diamond p \land \Diamond q) \]

(which is indeed true) then it must also be the case that

\[ \vdash Spec' \Rightarrow (\Diamond p \land \Diamond q). \]
Aside: The meaning of ‘⇒’

What does it mean when we say $\varphi \Rightarrow \psi$?

Recall that, models for our temporal formulae are of the form $\langle N, \pi \rangle$, representing

$$i-1 \quad i \quad i+1 \quad i+2$$

$\pi(i)$ $\pi(i+1)$

$p, q, s, w$ $p, s, t$

So, $\varphi \Rightarrow \psi$ means: for all $\pi$, if $\langle N, \pi \rangle \models \varphi$ then $\langle N, \pi \rangle \models \psi$.

Alternatively: the set of models that satisfy $\varphi$ is a subset of the set of models that satisfy $\psi$. 
So, when we say $Spec_2 \Rightarrow Spec_1$ this also means that

*models satisfying* $Spec_2 \subseteq$ *models satisfying* $Spec_1$.

So, refinements

$Spec_1$

$Spec_2$

$\ldots$

$\ldots$

$Spec_n$

are successively reducing the number of possible models (and so the set of possible execution sequences).
Example

\[ \text{Spec} = p \land \lozenge q \] has models such as

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]

\[ p \quad q \]
Linking Specifications

Consider a specification, $Spec_1$, for a program element $E_1$, together with another specification, $Spec_2$, for element $E_2$.

In programming languages, the elements can be executed together in a variety of ways (e.g. interleaved, concurrent).

In addition, the ways in which information can be passed between these elements should be identified (see later).

Note that, if no such communication occurs between elements, then they cannot have any significant effect on each other (though we may still be interested in the evolution of the combined system).

So, we must first decide upon, and describe, the form of concurrency and communication used in our systems.
Concurrenty

Throughout the following, we will assume we have several independent elements, $E_1, E_2, \ldots, E_n$.

These elements may be processes, objects, threads, agents, etc.

We will primarily tackle the simplest mechanism for combining elements, namely *synchronous true concurrency*.

Before we do this, we should recap what this means.

In the following, we will look at various alternatives, the choice of which can make a great deal of difference to the ease/difficulty of temporal specification.
Interleaving .vs. True Concurrency

- **True Concurrency** allows the elements to be executing at the same time, but independently:

  ![Diagram showing True Concurrency]

  - $E_1$
  - $E_2$

- **Interleaving** ensures that only one of the elements can execute at any one time.

  ![Diagram showing Interleaving]

  - $E_1$
  - $E_2$

Characterising interleaving:

$$\Box (\text{executing}(E_1) \lor \text{executing}(E_2)) \land \Box \neg (\text{executing}(E_1) \land \text{executing}(E_2))$$
Synchrony vs. Asynchrony

**Synchronous** execution ensures that all elements work on the same notion of *next moment* (shared clock).

![Diagram of synchronous execution]

**Asynchronous** execution allows the elements to work at different *speeds*.

![Diagram of asynchronous execution]

Again, we will mainly use *synchronous, true concurrency*, though we will explore other possibilities later.
Concurrency

We have

\( \text{Spec}_A \), a specification of element \( A \), and

\( \text{Spec}_B \), a specification of element \( B \).

Now, we want to specify the system comprising \( A \) and \( B \)

- executing \textit{concurrently}, and
- executing \textit{synchronously},
- but without any \textit{communication},

To do this, we simply conjoin the specifications, i.e.

\[ \text{Spec}_A \land \text{Spec}_B \]
Example: Specification

\[ Spec_A = a \land \circ b \land \circ \circ c \land \circ \circ \circ \circ (a \lor b) \]
\[ Spec_B = x \land \circ \circ y \land \circ \circ \circ \circ z \]

Then the synchronous, concurrent combination of A and B is

\[ Spec_A \land Spec_B = (a \land x) \land \circ b \land \circ \circ (c \land y) \land \circ \circ \circ \circ (z \land (a \lor b)) \]

Notice how, in the above example, there is no interaction between the propositions in \( Spec_A \), namely \( \{a, b, c\} \), and the propositions in \( Spec_B \), namely \( \{x, y, z\} \).
Example: Models/Executions (1)

When we consider models/executions over the alphabet \( \{a, b, c, x, y, z\} \), we note that a model for \( \text{Spec}_A \land \text{Spec}_B \) must be a model for both \( \text{Spec}_A \) and \( \text{Spec}_B \) separately.

Sample models of \( p \land \bigcirc q \) (over the alphabet \( \{p, q, r\} \)) are

\[
\begin{align*}
&\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \cdots \\
&p & q & \neg r & \neg r
\end{align*}
\]

\[
\begin{align*}
&\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \cdots \\
&p & q & r & \neg r
\end{align*}
\]
Sample models of $r \land \bigcirc \neg r$ (over the alphabet $\{p, q, r\}$) are

The only model for $(p \land \bigcirc q) \land (r \land \bigcirc \neg r)$ here is

If two formulae have models, and if there is no interaction between the alphabets, then the conjunction has a model.
Consider the possible models (or execution sequences) of each of these elements separately.

\[ E_1 = \begin{align*}
& x := 0; \\
& x := x + 1; \\
& x := 5; \\
& \text{end}
\end{align*} \]

\[ E_2 = \begin{align*}
& y := 7; \\
& y := y - 1; \\
& y := 0; \\
& \text{end}
\end{align*} \]

Sample models (over all variables, \(x\) and \(y\)) for \(E_1\) include:

\begin{itemize}
  \item \(x = 0, y = 7\)
  \item \(x = 1, y = 6\)
  \item \(x = 5, y = 0\)
  \item \(x = 0, y = 99\)
  \item \(x = 1, y = 98\)
  \item \(x = 5, y = 97\)
\end{itemize}

Notice how the values of \(x\) are constrained by the code of \(E_1\), while \(y\) is unconstrained.
Sample models (again over all variables, $x$ and $y$) for $E_2$ include:

Now, amongst all these, the only common model/execution for the synchronous, concurrent combination of $E_1$ and $E_2$ is: