Using Continuous Real Functions to Model Timed Histories

Brendan Mahony
Ian Hayes
Department of Computer Science
University of Queensland 4072
Australia

July, 1991

Abstract

Continuous real functions are an important tool in describing the evolution of physical processes through time. Using the theory of topology, this notion of continuity may be generalised to arbitrary data types. This paper demonstrates that (topological) continuity can be a useful tool in describing the evolution of digital processes through time. Several examples are given of the use of continuous functions in modeling and specifying system behaviour. A digital circuit is verified to demonstrate the utility of proof techniques from real analysis.

1 Introduction

In studying the dynamics of physical processes it is usual to model quantities as continuous real-valued functions of time. This paper demonstrates that continuous functions are also useful for studying the dynamics of digital systems. Our introduction to topology is brief, but sufficient to demonstrate its usefulness in real-time specification. The interested reader will find more extensive treatments of topology in [3, 4].

In Section 2 we overview the notion of topological continuity as a generalisation of real continuity. We then consider the standard topologies for the reals (Section 2.2) and for discrete spaces (Section 3), giving examples of the usefulness of functions that are continuous under these topologies.

We do not attempt to promote any particular specification style. Our examples are presented in an informal Z style since this is familiar to the authors. The purpose of the paper is to display the usefulness of continuity regardless of the specification method used. We restrict our definitions of notations to those that are directly related to the use of continuous functions in specifications. Other notations used are conventional either to the study of real numbers or to the Z specification language [5]. Informal definitions of these can be found in the glossary at the end of the paper.

2 Topology

Consider the definition of real continuity presented in elementary applied mathematics texts.

> A function, $f : \mathbb{R} \to \mathbb{R}$, is *continuous* at a point, $x : \mathbb{R}$, if
>
> $$\lim_{a \to x} f(a) = f(x).$$

The notion of limit is left vague, relying on the reader's intuition for the reals, and the fact that limits for many functions may be found by algebraic means.
A more rigorous definition appears in pure maths calculus texts.

> A function, $f : \mathbb{R} \to \mathbb{R}$ is *continuous* at a point, $x : \mathbb{R}$, if for every $\epsilon : \mathbb{R} > 0$ there is a $\delta : \mathbb{R} > 0$ such that
>
> $$\forall\, y : \mathbb{R} \bullet |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$$

Here the notion of limit has been formalised, but still the definition remains fundamentally bound to the real space. A generalisable definition may be given in terms of intervals around the continuity point.

> A function, $f : \mathbb{R} \to \mathbb{R}$ is *continuous* at a point, $x : \mathbb{R}$, if for every $\epsilon : \mathbb{R}$ there is a $\delta : \mathbb{R}$ such that
>
> $$\{y : \mathbb{R} \mid |x - y| < \delta\} \subseteq f^{-1}(\!|\{z : \mathbb{R} \mid |f(x) - z| < \epsilon\}|\!)$$
> or
> $$(\!|x - \delta \mathinner{..} x + \delta|\!) \subseteq f^{-1}(\!|(\!|f(x) - \epsilon \mathinner{..} f(x) + \epsilon|\!)|\!)$$

The notion of intervals can be generalised to arbitrary spaces. The study of such generalisations is called *topology*.

2.1 Open Sets

Topology uses the concept of *open* set to generalise real neighbourhoods to arbitrary spaces. Open sets are an expression of the contiguousness of elements of the space. Any open set containing a particular element must also contain some neighbourhood around that element. The granularity of these neighbourhoods determine the degree of contiguousness within the space, ranging from discrete (single element neighbourhoods) to analog (uncountable neighbourhoods).
A complete collection of open sets on a space is called a topology. Since any neighbourhood around a point in a space X is contained in the entire space, a topology on X must contain X itself. The union of two neighbourhoods should remain a neighbourhood, as should the intersection. A topology must be closed under arbitrary unions, but

only under finite intersections [3]. This allows new open sets to be constructed from known ones whilst ensuring that each point of the space carries some neighbourhood with it in each open set. Finally to ensure the topology is closed under intersection the null set must be included.

Definition 2.1

$$Topologies[X] == \left\{ \mathcal{T} : \mathbb{P}\,\mathbb{P}\,X \;\middle|\; \begin{array}{l} \{\}, X \in \mathcal{T} \\ \forall\, \mathcal{O} : \mathbb{F}\,\mathcal{T} \bullet \bigcap \mathcal{O} \in \mathcal{T} \\ \forall\, \mathcal{O} : \mathbb{P}\,\mathcal{T} \bullet \bigcup \mathcal{O} \in \mathcal{T} \end{array} \right\}$$

The topologies on a space can be used to generalise our definition of real continuity. A continuous function maps neighbouring points in its domain to neighbouring points in its range.

Definition 2.2 *For sets X and Y, with topologies $\mathcal{T}_X : Topologies[X]$ and $\mathcal{T}_Y : Topologies[Y]$, the continuous total functions and continuous partial functions are*

$$X \mathrel{\oplus\!\!\!\rightarrow} Y == \{f : X \to Y \mid (\forall\, O : \mathcal{T}_Y \bullet f^{-1}(\!| O |\!) \in \mathcal{T}_X)\}$$
$$X \mathrel{\oplus\!\!\!\!\rightarrow} Y == \{f : X \pfun Y \mid (\forall\, O : \mathcal{T}_Y \bullet f^{-1}(\!| O |\!) \in \mathcal{T}_X)\}$$

Under a continuous function the preimage of an open set is always open. The preimage is used because of the many-to-one nature of functions would make a direct image definition too restrictive. For example the range of sine is the closed interval $[-1 \,..\, 1]$. Definition 2.2 requires neighbouring points in the domain to be mapped to neighbouring points in the range, but does not require that all neighbouring points in the range be mapped to.
The continuous functions between two spaces depend on the topologies being used, but we do not make explicit reference to them since the topology being used is generally apparent from context.
We include the notion of partial functions, which is perhaps unusual for continuous functions, so as to avoid the necessity of knowing the precise domain of a function when typing it. The continuity criteria of respecting open sets readily admits the notion of partial functions.

2.2 The Real Topology

The real topology is constructed using the open intervals as a basis.

Definition 2.3

$$
\begin{array}{|l}
\llparenthesis \_ \ldots \_ \rrparenthesis : \mathbb{R} \times \mathbb{R} \nrightarrow \mathbb{P}\,\mathbb{R} \\
\llparenthesis -\infty \ldots \_ \rrparenthesis, \llparenthesis \_ \ldots \infty \rrparenthesis : \mathbb{R} \rightarrow \mathbb{P}\,\mathbb{R} \\
\llparenthesis -\infty \ldots \infty \rrparenthesis : \mathbb{P}\,\mathbb{R} \\
\hline
\forall\, x, y : \mathbb{R} \bullet \\
\quad \llparenthesis x \ldots y \rrparenthesis = \{ z : \mathbb{R} \mid x < z < y \} \\
\quad \llparenthesis -\infty \ldots x \rrparenthesis = \{ z : \mathbb{R} \mid z < x \} \\
\quad \llparenthesis x \ldots \infty \rrparenthesis = \{ z : \mathbb{R} \mid x < z \} \\
\quad \llparenthesis -\infty \ldots \infty \rrparenthesis = \mathbb{R}
\end{array}
$$

An open set on the reals is constructed from arbitrary unions and finite intersections of open intervals.

Definition 2.4

$$
\mathfrak{I}_{\mathbb{R}} == \begin{array}{l}
\{ \llparenthesis x \ldots y \rrparenthesis \mid x, y : \mathbb{R} \} \cup \\
\{ \llparenthesis -\infty \ldots x \rrparenthesis \mid x : \mathbb{R} \} \cup \\
\{ \llparenthesis x \ldots \infty \rrparenthesis \mid x : \mathbb{R} \} \cup \\
\{ \llparenthesis -\infty \ldots \infty \rrparenthesis \}
\end{array}
$$

$$
\mathcal{T}_{\mathbb{R}} == \{ \bigcup O \mid O : \mathbb{P}\, \mathfrak{I}_{\mathbb{R}} \} \cup \{ \bigcap O \mid O : \mathbb{F}\, \mathfrak{I}_{\mathbb{R}} \}
$$

2.3 Covering Open Sets of Reals

This topology has the following useful property.

Theorem 2.5 [4, Prop 8, page 39] *Every open set of real numbers is the union of a countable collection*[†] *of disjoint open intervals.*

Corollary 2.6 *The function*

$$
\begin{array}{|l}
\mathrm{cov} : \mathcal{T}_{\mathbb{R}} \rightarrow \mathbb{P}_{\omega}\, \mathfrak{I}_{\mathbb{R}} \\
\hline
\forall\, O : \mathcal{T}_{\mathbb{R}} \bullet \\
\quad \{\} \notin \mathrm{cov}(O) \\
\quad O = \bigcup \mathrm{cov}(O) \\
\quad \forall\, A, B : \mathrm{cov}(O) \bullet A \neq B \Rightarrow A \cap B = \{\}
\end{array}
$$

is uniquely defined.

It is this property of the real topology that allows real continuity to be defined in terms of open intervals only. It also allows many propositions about continuous functions to be stated in terms of open intervals.
For example consider a control system that must ensure that the temperature,

$$\theta : TIME \nrightarrow TEMP$$

[†] We write $\mathbb{P}_{\omega}\, X$ for the set of countable subsets of X.

(where both $TIME$ and $TEMP$ are the positive reals, $\mathbb{R}_+$) of a computer machine room, does not remain above a certain threshold, $\theta_{max} : TEMP$, for too long, say not longer than $\delta : TIME$. This condition on the temperature function may be stated easily by considering the duration of the time intervals for which the temperature is too high. Since θ is a continuous function, the preimage of the interval $(\theta_{max} \ldots \infty)$, the dangerous temperatures, is an open set. This means that the times at which the temperature is dangerous can be expressed as the set of maximal open intervals, $\mathrm{cov}(\theta^{-1}(\!|(\theta_{max} \ldots \infty)|\!))$. Each of these intervals must be of short duration.

$$\forall \Delta : \mathrm{cov}(\theta^{-1}(\!|(\theta_{max} \ldots \infty)|\!)) \bullet \|\Delta\| < \delta$$

An example of the behaviour allowed by this specification is shown in Figure 1. Each interval for which the temperature rises above the threshold θ_{max} must have duration less than δ.

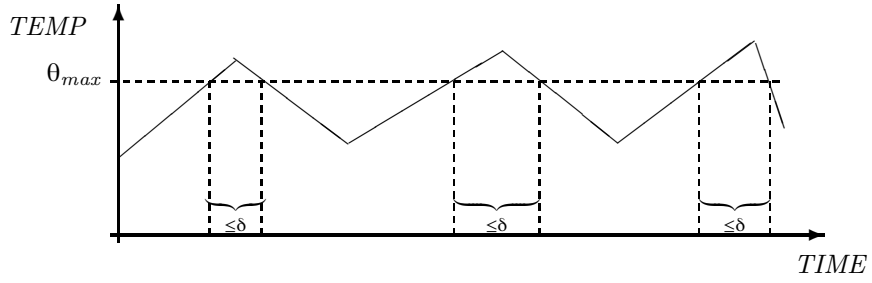

Figure 1: An example behaviour of the temperature control system.

3 Discrete Topologies

When the space under consideration is countable, it is usual to give a topology in which each individual point is an open set. This is called a *discrete* topology. Since topologies must be closed under unions the discrete topology is just the space's power set.

Definition 3.1 *For a space, X, the* discrete *topology is the collection of all subsets of X.*

$$\mathcal{D}_X == \mathbb{P}\, X$$

The interesting aspect of the discrete topology is that continuous functions from the reals (time) into a discrete space are step functions (see Figure 2). The preimage of a point in the discrete space must be an open set of reals, that is a set of open intervals. This means that when such a function has a value at a particular point it must have the same value for the entirety of some interval around that point. In order to change value

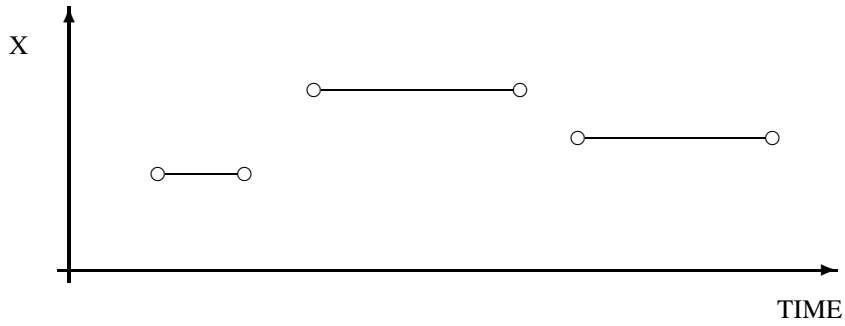

Figure 2: An example of a continuous partial function into a discrete space.

it must become undefined for some interval. This is a good way to model the history of a digital quantity that remains constant, unless acted on by an event.
For example the behaviour of a digital wire may be represented as a continuous partial function of time.

$$WIRE : TIME \pfun \{hi, lo\}$$

By defining the behaviour to be continuous we remove pathological behaviour, such as the wire being hi on the rationals and lo on the irrationals. Continuity forces a *discrete* nature on the behaviours.
Having continuous behaviours also means that we can associate events with "discontinuities" in the behaviour. We can characterise important events such as

$$GoesHi == WIRE(t_0) = lo \land WIRE(t_1) = hi \land t_0 < t_1$$

and identify the periods during which these events occur.
A state change occurs when there is an interval of time, Δ, when the $WIRE$ is undefined. The $WIRE$ $GoesHi$ during Δ if

$$\begin{array}{l} \Delta \subseteq TIME \setminus \mathrm{dom}\ WIRE \\ \exists\, \Delta_{lo}, \Delta_{hi} : \mathrm{cov}(\mathrm{dom}\ WIRE) \bullet \\ \quad \sup \Delta_{lo} = \inf \Delta \land \inf \Delta_{hi} = \sup \Delta \\ \quad \forall\, t_0 : \Delta_{lo};\ t_1 : \Delta_{hi} \bullet GoesHi \end{array}$$

Figure 3 shows an example of an interval over which the $GoesHi$ event is occurring. The wire is low for times immediately preceding the event and high for those immediately following it.
In this way we are able to give a formal correspondence between event-based views of process behaviour and state-based views.
Our ideal digital wire also has direct correspondence to real-world analog wires. An analog wire can be described by a real-valued continuous total function of time (we may be representing either voltage or current).

$$AWIRE : TIME \pfun \mathbb{R}$$

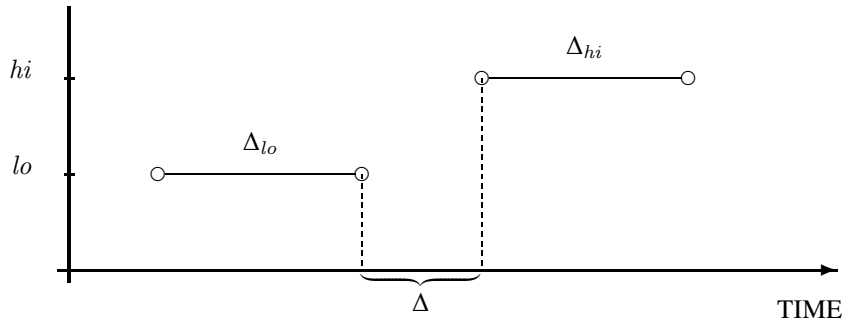

Figure 3: A $GoesHi$ event occurs at Δ.

The digital information is derived from the analog wire by defining a high threshold, $\alpha : \mathbb{R}$, above which the signal is considered high, and low threshold, $\beta : \mathbb{R}$, $\beta \leq \alpha$, below which the signal is considered low. Between these two values the signal is undetermined. The correspondence between the analog wire and the digital wire is simple.

$$WIRE(t) = hi \Leftrightarrow AWIRE(t) > \alpha \wedge$$
$$WIRE(t) = lo \Leftrightarrow AWIRE(t) < \beta$$

If $AWIRE$ is continuous then $WIRE$ will also be continuous.

$$\{t : \mathbb{R} \mid AWIRE(t) > \alpha\} = AWIRE^{-1}(\!(\{\alpha \mathinner{..} \infty\})\!)$$

is open by the continuity of $AWIRE$. This set is the preimage of hi under $WIRE$. Similarly the preimage of lo under $WIRE$ is open, and hence $WIRE$ is continuous.
It is also possible to move to a sampled bitstream view of $WIRE$. Suppose a sampling device monitors $WIRE$ over periods of duration, $\delta : TIME$, returning 1 if $WIRE$ is hi over the entire period, 0 if it is was lo, and $\perp$ otherwise. The sampled bitstream, $BITS : \text{seq}\{\perp, 0, 1\}$, has simple relationship to the digital $WIRE$.

$$\begin{aligned} & BITS(i) = 1 \wedge (\!(\{(i-1).\delta \mathinner{..} i.\delta\})\!) \subseteq WIRE^{-1}(\!(\{hi\})\!) \\ \vee\ & BITS(i) = 0 \wedge (\!(\{(i-1).\delta \mathinner{..} i.\delta\})\!) \subseteq WIRE^{-1}(\!(\{lo\})\!) \\ \vee\ & BITS(i) = \perp \wedge \neg \left(\begin{array}{l} (\!(\{(i-1).\delta \mathinner{..} i.\delta\})\!) \subseteq WIRE^{-1}(\!(\{hi\})\!) \\ \vee\ (\!(\{(i-1).\delta \mathinner{..} i.\delta\})\!) \subseteq WIRE^{-1}(\!(\{lo\})\!) \end{array} \right) \end{aligned}$$

By using continuous functions we are able to switch between different levels of abstraction, whilst retaining complete rigor.

4 The ‘on’ Operator

The preimage notation used to define $BITS$ above is cumbersome, especially as it is common to discuss behaviour over entire time intervals. To abbreviate the expression

of such properties we introduce the on operator. If $P(t)$ is a predicate in which a time variable t occurs free, we write P on O, dropping all references to t, to express that P is defined and true for all times in O. For example the definition of $BITS$ might be more conveniently expressed using the on notation.

$$\begin{array}{l} \quad BITS(i) = 1 \land (WIRE = hi) \text{ on } (\!|(i-1).\delta \mathinner{..} i.\delta|\!) \\ \lor\ BITS(i) = 0 \land (WIRE = lo) \text{ on } (\!|(i-1).\delta \mathinner{..} i.\delta|\!) \\ \lor\ BITS(i) = \bot \land \neg \left(\begin{array}{l} WIRE = hi \text{ on } (\!|(i-1).\delta \mathinner{..} i.\delta|\!) \\ \lor\ WIRE = lo \text{ on } (\!|(i-1).\delta \mathinner{..} i.\delta|\!) \end{array} \right) \end{array}$$

5 Example: A Nor Gate

A nor gate calculates the negation of the logical disjunction of two digital wires. This process cannot be achieved without some delay in the signal. The best that is possible is that the delay be within some time interval, $(\!|\delta_2 \mathinner{..} \delta_1|\!)$. The upper bound $\delta_1 : TIME$ ensures that the nor gate is sufficiently responsive, whilst the lower bound $\delta_2 : TIME$ ensures that the delayed signal is not cut too short. If the input signals are carried by wires a and b, and the output by c then c should be set low if either a or b are high and it should be set high if both are low.

NorGate

$$a, b, c : TIME \pfun \{hi, lo\}$$

$$\begin{array}{l} \forall x, y : TIME \bullet \\ \quad (a = hi \lor b = hi) \text{ on } (\!|x \mathinner{..} y|\!) \Rightarrow c = lo \text{ on } (\!|x + \delta_1 \mathinner{..} y + \delta_2|\!) \\ \quad (a = lo \land b = lo) \text{ on } (\!|x \mathinner{..} y|\!) \Rightarrow c = hi \text{ on } (\!|x + \delta_1 \mathinner{..} y + \delta_2|\!) \end{array}$$

6 Example: Verifying a Flipflop

In using continuous real functions, not only are we able to use familar models for physical processes, we are also able to bring to bear the large body of knowledge in the field of real analysis. We show how one technique from real analysis can be used to help verify the behaviour of a flipflop.

6.1 Real Induction

As with the natural numbers induction is an important way of showing that some property holds over an interval of real numbers. The real version of induction relies on being able to show the property is satisfied on a small interval (the initial case) and then showing that the property holding for one real number implies it holds for some slightly larger number (the inductive case). The intuition is that the inductive case allows the interval of satisfaction to be extended from the small initial interval, one small interval at a time to the required interval.

Definition 6.1 (Principle of Real Induction)
For $\delta : \mathbb{R} > 0$,

$$\frac{P \text{ on } (a \mathinner{..} a + \delta] \quad \forall z : (a \mathinner{..} c) \bullet P(z) \Rightarrow P(z + \delta)}{P \text{ on } (a \mathinner{..} c + \delta)}$$

6.2 A Bit

A bit stores a single binary digit, constantly providing the value of the digit on a line Q. The value of the bit is set to lo by sending a hi signal on a reset line R, while maintaining a lo signal on a set line S. Once reset the value of the bit should remain lo for as long as the set signal is lo. The value of the bit may be set hi via a similar process, except with the hi signal on S and the lo on R.

Bit

$$R, S, Q : TIME \pfun \{hi, lo\}$$

$$\begin{array}{l}
\forall x, y, z : TIME \bullet \\
\quad x + \delta_s < y < z \Rightarrow \\
\qquad R = hi \text{ on } (x \mathinner{..} y) \land S = lo \text{ on } (x \mathinner{..} z) \Rightarrow \\
\qquad\quad Q = lo \text{ on } (x + \delta_\uparrow \mathinner{..} z + \delta_\downarrow) \\
\qquad S = hi \text{ on } (x \mathinner{..} y) \land R = lo \text{ on } (x \mathinner{..} z) \Rightarrow \\
\qquad\quad Q = hi \text{ on } (x + \delta_\uparrow \mathinner{..} z + \delta_\downarrow)
\end{array}$$

The bit need only respond to signals that are stable for $\delta_s : TIME$. It is expected that there will be some delay in the Bit responding to variations in the set and reset signals. This delay should be no more than $\delta_\uparrow : TIME$ and no less than $\delta_\downarrow : TIME < \delta_\uparrow$.

6.3 A Flipflop Implements a Bit

A flipflop may be constructed using two nor gates, with maximum and minimum response delays δ_1 and $\delta_2 < \delta_1$, by connecting the output of each gate to one input of the other as shown in Figure 4.

$$FlipFlop == NorGate[\tfrac{S}{a}, \tfrac{Q}{b}, \tfrac{\overline{Q}}{c}] \land NorGate[\tfrac{\overline{Q}}{a}, \tfrac{R}{b}, \tfrac{Q}{c}]$$

A possible behaviour for a *FlipFlop* is shown in Figure 5.
We begin verifying *FlipFlop* by showing that it is stable after set and reset.

Theorem 6.2 (Reset Stability)
For a FlipFlop, if $S = lo$ on $(x \mathinner{..} y]$ *for some* $x, y : \mathbb{R}$ *and* $(Q = lo \land (R = hi \lor \overline{Q} = hi))$ on $(x \mathinner{..} x + \delta_1]$ *then*

$$(Q = lo \land \overline{Q} = hi) \text{ on } (x + \delta_1 \mathinner{..} y + \delta_2].$$

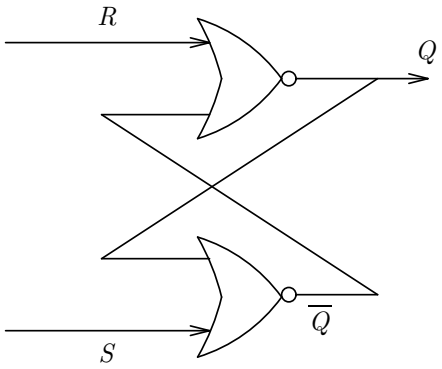

Figure 4: Circuit diagram for a nor gate flipflop.

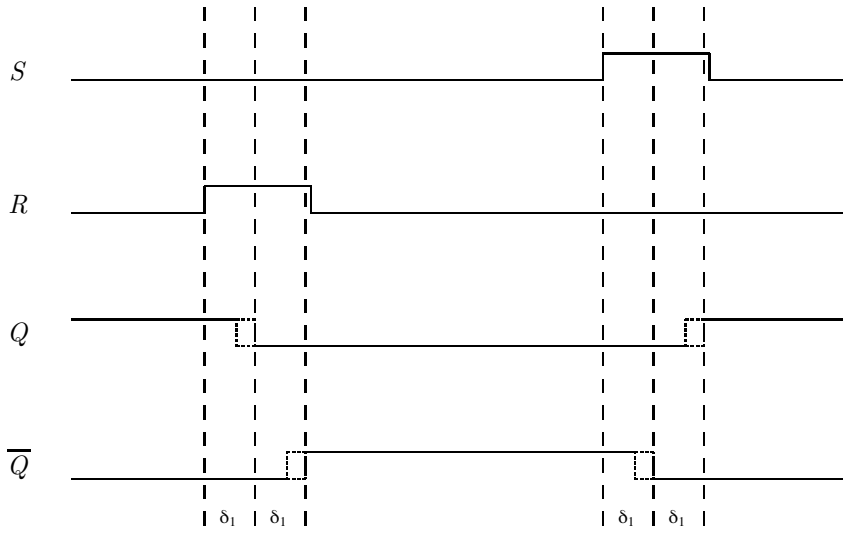

Figure 5: An example behaviour of a flipflop.

Proof: We use the principle of real induction on the proposition,

$$P == \left(\begin{array}{l} \lambda\, z : \mathit{TIME} \bullet \\ \quad Q = lo \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \wedge \\ \quad (R = hi \vee \overline{Q} = hi) \text{ on } (\!\!\{x \mathinner{..} x + \delta_1\}\!\!] \wedge \\ \quad \overline{Q} = hi \text{ on } (\!\!\{x + \delta_1 \mathinner{..} z + \delta_1\}\!\!] \end{array} \right)$$

If we show that P on $(\!\!\{x \mathinner{..} (y + \delta_2) - \delta_1\}\!\!)$ then we can deduce that

$$\begin{array}{l} (Q = lo \wedge \overline{Q} = hi) \text{ on } (\!\!\{x + \delta_1 \mathinner{..} (y + \delta_2) - \delta_1 + \delta_1\}\!\!] \\ \equiv (Q = lo \wedge \overline{Q} = hi) \text{ on } (\!\!\{x + \delta_1 \mathinner{..} y + \delta_2\}\!\!] \end{array}$$

We will prove the proposition using the inductive constant δ_2. We find it convenient to prove the inductive step and derive the initial step from it.

Case (Inductive Step)

Since we wish to show the proposition on $(\!\!\{x \mathinner{..} (y - \delta_1) + \delta_2\}\!\!)$, we choose an arbitrary $z : (\!\!\{x \mathinner{..} y - \delta_1\}\!\!)$ and assume that $P(z)$ holds, i.e.,

$$\begin{array}{l} Q = lo \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \wedge \\ (R = hi \vee \overline{Q} = hi) \text{ on } (\!\!\{x \mathinner{..} x + \delta_1\}\!\!] \wedge \\ \overline{Q} = hi \text{ on } (\!\!\{x + \delta_1 \mathinner{..} z + \delta_1\}\!\!] \\ \Rrightarrow\ Q = lo \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \wedge \\ \quad (R = hi \vee \overline{Q} = hi) \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \end{array}$$

By assumption we know also that

$$S = lo \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!].$$

By the definition of $\mathit{FlipFlop}$[†],

$$\begin{array}{l} (R = hi \vee \overline{Q} = hi) \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \Rrightarrow \\ \quad Q = lo \text{ on } (\!\!\{x + \delta_1 \mathinner{..} (z + \delta_1) + \delta_2\}\!\!] \end{array}$$

so that

$$\begin{array}{l} Q = lo \text{ on } ((\!\!\{x \mathinner{..} x + \delta_1\}\!\!] \cup (\!\!\{x + \delta_1 \mathinner{..} z + \delta_1 + \delta_2\}\!\!]) \\ \equiv Q = lo \text{ on } (\!\!\{x \mathinner{..} (z + \delta_2) + \delta_1\}\!\!]. \end{array}$$

Also by $\mathit{FlipFlop}$ we know that

$$(Q = lo \wedge S = lo) \text{ on } (\!\!\{x \mathinner{..} z + \delta_1\}\!\!] \Rrightarrow \overline{Q} = hi \text{ on } (\!\!\{x + \delta_1 \mathinner{..} (z + \delta_1) + \delta_2\}\!\!]$$

so that

$$\begin{array}{l} \overline{Q} = hi \text{ on } ((\!\!\{x + \delta_1 \mathinner{..} z + \delta_1\}\!\!] \cup (\!\!\{z + \delta_1 \mathinner{..} z + \delta_1 + \delta_2\}\!\!]) \\ \Rrightarrow \overline{Q} = hi \text{ on } (\!\!\{x + \delta_1 \mathinner{..} (z + \delta_2) + \delta_1\}\!\!] \end{array}$$

Thus it follows that $P(z + \delta_2)$ holds.

[†]Note that for $f : \mathit{TIME} \nrightarrow A$, $c : A$, $a, b : \mathit{TIME}$, A discrete, since $f^{-1}(\!|\{c\}|\!)$ is open, then $f = c$ on $(\!\!\{a \mathinner{..} b\}\!\!]$ iff there is some $\Delta : \mathrm{cov}(f^{-1}(\!|\{c\}|\!))$, such that $(\!\!\{a \mathinner{..} b\}\!\!] \subseteq \Delta$, that is iff there exists some $\epsilon : \mathit{TIME} > 0$ such that $f = c$ on $(\!\!\{a \mathinner{..} b + \epsilon\}\!\!)$.

Case (Initial Step)
It is easy to show that $P(z) \Rightarrow P$ on $(x \mathinner{..} z]$. Now $P(x)$ holds by assumption. From the above argument we know that $P(x + \delta_2)$ must also hold, so that P on $(x \mathinner{..} x + \delta_2]$.

So by the principle of real induction we may deduce that P on $(x \mathinner{..} (y + \delta_2) - \delta_1)$, and hence that proposition holds. □

Corollary 6.3 (Reset Validity)
For a FlipFlop, if for some $x + 2\delta_1 < y < z : \mathbb{R}$,
$R = hi$ on $(x \mathinner{..} y)$ $\wedge$ $S = lo$ on $(x \mathinner{..} z)$ *then*

$$(Q = lo \wedge \overline{Q} = hi) \text{ on } (x + 2\delta_1 \mathinner{..} z + \delta_2).$$

Proof: Since $R = hi$ on $(x \mathinner{..} x + 2\delta_1]$ the definition of *FlipFlop* ensures that $(R = hi \wedge Q = lo)$ on $(x + \delta_1 \mathinner{..} x + 2\delta_1]$ and the results follows from the stability theorem. □

Theorem 6.4 (Set Stability)
In a FlipFlop system, if $R = lo$ on $(x \mathinner{..} y]$ *for some* $x, y : \mathbb{R}$ *and* $(\overline{Q} = lo \wedge (S = hi \vee Q = hi))$ on $(x \mathinner{..} x + \delta_1]$ *then*

$$(Q = hi \wedge \overline{Q} = lo) \text{ on } (x + \delta_1 \mathinner{..} y + \delta_2].$$

Proof: The proof is similar to that for reset stability. □

Corollary 6.5 (Set Validity)
For a FlipFlop, if for some $x + 2\delta_1 < y < z : \mathbb{R}$,
$S = hi$ on $(x \mathinner{..} y)$ $\wedge$ $R = lo$ on $(x \mathinner{..} z)$ *then*

$$(Q = hi \wedge \overline{Q} = lo) \text{ on } (x + 2\delta_1 \mathinner{..} z + \delta_2).$$

From Corollaries 6.3 and 6.5 we may deduce that *FlipFlop* produces a valid refinement of Bit.

Theorem 6.6 *If* $\delta_\downarrow < \delta_2$, $2.\delta_1 < \delta_\uparrow$, *and* $2.\delta_1 < \delta_s$, *then*

$$FlipFlop \Rightarrow Bit$$

7 Conclusions

A small working knowledge of topology can prove a powerful tool in the specification and design of real-time systems. Topologically continuous functions offer a convenient model for the history of observable quantities, both analog and digital. They allow one a high degree of confidence that the specified behaviour will indeed correlate to the physical behaviour of the system described. Yet, continuous functions have sufficient structure to allow complex specifications to be written clearly and succinctly. There is little difference in expressive power between using discrete continuous functions and say sequences to model histories of digital behaviour. Further, formal analysis techniques for real continuous functions are both powerful and well understood so that this model is also comparable when deriving properties from specifications.
The use of continuous history functions allows the transparent integration of both analog and digital quantities in a real-time specification. Analog quantities are modelled in the conventional engineering manner, by continuous real-valued functions of time. By representing digital quantities as (topologically) continuous functions of time, all quantities are thus put into the single framework of continuous history functions.
This has been exploited in [1] to produce a high-level specification of the thermodynamic behaviour of a central heating system and then to verify the correct behaviour of a digital control mechanism. The specification technique used in [1] is a generalisation of the specification statements of Morgan [2], but continuous history functions should prove equally useful with other specification methods.

References

[1] B. P. Mahony and I. J. Hayes. A case-study in real-time specification: A central heater. In *The BCS FACS Fourth Refinement Workshop*. Springer-Verlag, 1991.

[2] C. C. Morgan, K. A. Robinson, and P. Gardiner. On the refinement calculus. Technical Monograph PRG-70, Oxford University Programming Research Laboratory, 1988.

[3] J. R. Munkres. *Topology A First Course*. Prentice-Hall, Inc., 1975.

[4] H. L. Royden. *Real Analysis*. Macmillan Publishing Co., Inc., second edition, 1968.

[5] J. M. Spivey. *The Z Notation: A Reference Manual*. Prentice Hall International, 1989.

Glossary

Let x and y be real numbers, Δ a real interval, A and B sets, f a function, $\mathcal{A}$ a collection of sets, and P and Q are predicates.

$\mathbb{R}$	the set of real numbers
$\mathbb{R}_+$	the set of non-negative real numbers
$(x \mathinner{..} y)$	open interval from x to y
$(x \mathinner{..} y]$	half open interval from x to y, including y
$\lvert x \rvert$	magnitude of x
$\lVert \Delta \rVert$	the length of Δ
$\inf \Delta$	the greatest lower bound of Δ
$\sup \Delta$	the least upper bound of Δ
$A \to B$	total functions from A to B
$A \pfun B$	partial functions from A to B
$A \cfun B$	continuous total functions from A to B
$A \cpfun B$	continuous partial functions from A to B
$f(\!\lvert A \rvert\!)$	the image of A under the function f
P on O	P is true at all times in O
$\mathbb{P}\, A$	the subsets of A
$\mathbb{F}\, A$	the finite subsets of A
$\mathbb{P}_\omega\, A$	the countable subsets of A
$\bigcup \mathcal{A}$	the union of all the sets in the collection $\mathcal{A}$
$\bigcap \mathcal{A}$	the intersection of all the sets in the collection $\mathcal{A}$
$P \Rrightarrow Q$	$P \Rightarrow Q$ is valid