SOFTWARE VERIFICATION RESEARCH CENTRE

SCHOOL OF INFORMATION TECHNOLOGY

THE UNIVERSITY OF QUEENSLAND

Queensland 4072
Australia

TECHNICAL REPORT

No. 99-36

Induction in the Timed Interval Calculus

Axel Wabenhorst

Version 1.1, December 1999

Phone: +61 7 3365 1003
Fax: +61 7 3365 1533
http://svrc.it.uq.edu.au

Induction in the Timed Interval Calculus

Axel Wabenhorst

Abstract

The Timed Interval Calculus, a timed-trace formalism based on set theory, is introduced. It is extended with an induction law and a unit for concatention, which facilitates the proof of properties over trace histories. The effectiveness of the extended Timed Interval Calculus is demonstrated via a benchmark case study, the mine pump. Specifically, a safety property relating to the operation of a mine shaft is proved, based on an implementation of the mine pump and assumptions about the environment of the mine.

1 Introduction

One successful approach to modelling real-time systems has been via the representation of physical variables as functions which vary over time. Examples include the *Duration Calculus* (DC) [11, 12], the *Temporal Agent Model* [10] and, more recently, *Temporal Algebra* [4] and the *Timed Interval Calculus (TIC)* [2]. These languages are used to express and reason about dynamic properties of variables. They and their predecessors [7] showed how concatenation of time intervals can form the basis of an effective real-time modelling and reasoning capability.

TIC and DC differ in that TIC is founded in set theory, while DC is logic-based. In addition, DC does not distinguish between predicates which are the same "almost everywhere", whereas in TIC, predicates are distinguished even if they are different at only one point in time.

Section 2 presents the syntax and semantics of the Timed Interval Calculus. TIC is extended with a unit for concatenation and temporal operators $\Box$ ("always") and $\Diamond$ ("sometime"). In addition, transformation laws for the Calculus are presented, in particular a new induction law which facilitates reasoning over trace histories.

Section 3 discusses the specification and verification of the mine pump case study [1, 5] in the Timed Interval Calculus. This case study is sufficiently complex to render the verification of its safety properties a challenge, and is therefore seen as a benchmark case study. We provide a complete formal proof and motivate the proof strategy wherever possible, so that the reader might gain an intuition about how to approach such a proof in an analogous situation.

Liu [5] has also provided a specification and verification of the mine pump using the Duration Calculus. That approach assumes that the mine pump has the capacity to reduce the water level in the mine below danger within a fixed time period regardless of how high the water level is initially. Thus, it is not necessary to specify an initial condition and induction over trace histories is not required. As a result, the proof is greatly simplified. Our analogous constraint, condition 11, is weaker (and more realistic) in that it only assumes a minimum rate of water outflow once the pump has been switched on. Another previous approach [6] to the mine pump example contains only informal proofs and stipulates stricter conditions for the pump, so that there are no delays between detection of high water levels and low methane, and no flags.

Conclusions are drawn in Section 4.

2 Notation and Laws for Timed-Trace Predicates

The Timed Interval Calculus is a simple set-theoretic notation for concisely expressing properties of time intervals [2]. We present the existing foundations, the extensions and transformation laws.

2.1 Time

Let $\mathbb{T}$ be the time domain, denoting the real numbers $\mathbb{R}$. Time intervals will be specified as real intervals: for $a, z : \mathbb{T}$ with $a < z$, the left-open, right-closed interval between a and z is

$$(a \ldots z] \quad \widehat{=} \quad \{t : \mathbb{T} \mid a < t \leq z\}\,.$$

Similarly for left and right-open $(a \ldots z)$, left and right-closed $[a \ldots z]$, and left-closed, right-open $[a \ldots z)$ endpoint brackets. For left and right-closed intervals, we also allow $a = z$, so that a single point is a special case. However, the empty set is not an interval. The set $\mathbb{I}$ is the set of all (finite) non-empty time intervals just defined.

We reason about real-time systems by considering predicates on variables which vary with time. Thus, variables have the form $v : \mathbb{T} \to V$. For example, $H_2O : \mathbb{T} \to \mathbb{R}$ might represent the water level in a mine shaft. So the property that the water level is greater than some danger level $DangerH_2O$ at time t is expressed by $H_2O(t) > DangerH_2O$. Since $DangerH_2O$ is a constant, it may be considered as a constant function over time, so the property may be expressed as $H_2O(t) > DangerH_2O(t)$, or $(H_2O > DangerH_2O)(t)$. Therefore, the property that the water level is greater than the danger level is a function, the truth value of which varies over time: $H_2O > DangerH_2O : \mathbb{T} \to \mathbb{B}$. Thus, predicates can be considered to be functions $P : \mathbb{T} \to \mathbb{B}$.

2.2 Sets of Time Intervals

We now introduce the set of all time intervals during which some predicate is true everywhere [2, 6], which will be used to reason about real-time systems.

To increase the expressiveness of the reasoning, we permit the specification of features of the intervals themselves, specifically their infimum α, supremum ω, and duration $\delta = \omega - \alpha$. Thus, we allow free occurences of α and ω (and therefore δ in predicates. In this case, predicates are functions $\mathbb{T}^3 \to \mathbb{B}$, depending on t, α and ω. For instance, the property that the water level in a mine shaft is greater than the danger level for a period of at least one time unit is expressed by

$$H_2O > DangerH_2O \ \wedge \ \delta \geq 1.$$

Sets of time intervals are expressed by special brackets as follows.

Definition 1 (Sets of time intervals) *For a predicate $P : \mathbb{T}^3 \to \mathbb{B}$, we define the left-open, right-closed intervals where P holds as*

$$(\!\!\!-P-\!\!\!] \mathrel{\widehat{=}} \{(\alpha \ldots \omega] \mid \alpha, \omega : \mathbb{T} \ \wedge \ \alpha < \omega \ \wedge \ \forall\, t : (\alpha \ldots \omega] \ P(t, \alpha, \omega)\}.$$

The abbreviation $\delta \mathrel{\widehat{=}} \omega - \alpha$ is often made. Defined similarly are the left and right-open $(\!\!\!-P-\!\!\!)$, the left-closed, right-open $[\!\!\!-P-\!\!\!)$, and, with the condition $\alpha \leq \omega$ instead of $\alpha < \omega$, the left and right-closed $[\!\!\!-P-\!\!\!]$ brackets. Define right-open intervals

$$[\![\!\!\!-P-\!\!\!) \quad \widehat{=} \quad [\!\!\!-P-\!\!\!) \cup (\!\!\!-P-\!\!\!)\,,$$

similarly for sets of right-closed $[\![\!\!\!-P-\!\!\!]$, left-open $(\!\!\!-P-\!\!\!]\!]$, and left-closed $[\!\!\!-P-\!\!\!]\!]$ intervals. Define

$$[\![\!\!\!-P-\!\!\!]\!] \quad \widehat{=} \quad (\!\!\!-P-\!\!\!) \cup [\!\!\!-P-\!\!\!] \cup (\!\!\!-P-\!\!\!] \cup [\!\!\!-P-\!\!\!)\,.$$

□

Subsequently, we will state examples and laws using particular brackets, but in many cases there are analogous results with different bracketing which we omit for brevity.

While predicate P may contain free occurrences of α and ω, these variables are bound in $(\!\!\!-P-\!\!\!]$.

For example,

$$\begin{array}{cl} & (\!\!\!-H_2O \geq DangerH_2O \ \wedge \ \delta \geq 1-\!\!\!) \\ = & \{(\alpha \ldots \omega) \mid \alpha, \omega : \mathbb{T} \ \wedge \ \omega - \alpha \geq 1 \\ & \qquad\qquad\qquad\qquad \wedge \ \forall\, t : (\alpha \ldots \omega) \ H_2O(t) > DangerH_2O\}. \end{array}$$

is the set of all open intervals of length at least one, during which the water level is above the danger mark.

2.3 The Concatenation Operator

Since properties are expressed as sets of time intervals, conventional set operators can be used for manipulating them. However, it is often useful to connect intervals end-to-end, in order to reason about sequences of behaviours. In the Duration Calculus, this is achieved by the chop operator, denoted by $\frown$ [3, 11] or ; [5, 8]. We use a similar operator, called *concatenation* and denoted by ; [2]. However, unlike previously, we allow concatenation with the set $\{\varnothing\}$. While the empty set is not a time interval, we will see shortly that it is useful to reason with. It will be so useful, in fact, that we make two special definitions:

$$\begin{array}{ccc} \mathbf{1} & \mathrel{\widehat{=}} & \{\varnothing\} \\ \overline{S} & \mathrel{\widehat{=}} & S \cup \mathbf{1} \end{array}$$

where $S : \mathbb{P}\,\mathbb{I}$, and $\mathbb{P}$ denotes the powerset operator.

Definition 2 (Concatenation) *Let* X, $Y : \mathbb{P}\,\mathbb{I} \cup \{\mathbf{1}\}$. *Then*

$$X \mathbin{;} Y \mathrel{\widehat{=}} \{x \cup y \mid x : X \wedge y : Y \;\wedge\; x \cup y : \overline{\mathbb{I}} \;\wedge\; \forall\, t_1 : x \;\; \forall\, t_2 : y \quad t_1 < t_2\}.$$

□

Thus, $X \mathbin{;} Y : \mathbb{P}\,\mathbb{I} \cup \{\mathbf{1}\}$. If X, $Y : \mathbb{P}\,\mathbb{I}$, then an interval $x : X$ can be joined to an interval $y : Y$ to form a new interval $x \cup y$, if x occurs strictly before y, and the two intervals meet exactly with no overlap or gap. If there are no such intervals, then $X \mathbin{;} Y = \varnothing$; in any case, $X \mathbin{;} Y : \mathbb{P}\,\mathbb{I}$. If $X : \mathbb{P}\,\mathbb{I}$, then $X \mathbin{;} \mathbf{1} = \mathbf{1} \mathbin{;} X = X$, and $\mathbf{1} \mathbin{;} \mathbf{1} = \mathbf{1}$. Thus, $\mathbf{1}$ is the unit of sequential composition in $\mathbb{P}\,\mathbb{I} \cup \{\mathbf{1}\}$.

It is useful to be able to express the condition that a property P holds somewhere in a given interval. In the Duration Calculus, the property that P holds on a subinterval of a given interval is expressed by $\Diamond P$, defined to be $true \frown P \frown true$ [11]. Observe that concatenation with respect to two non-empty intervals returns an interval which is not a point. Therefore, $\llbracket true \rrbracket ; \llbracket P \rrbracket ; \llbracket true \rrbracket$ does not express the property that "P holds somewhere" in the case where the interval is a point. In addition, it excludes the possibility that P holds only at the left or right endpoint of an interval. Thus, rather than making the definition

$$\llbracket \Diamond P \rrbracket \mathrel{\widehat{=}} (\llbracket true \rrbracket \mathbin{;} \llbracket P \rrbracket \mathbin{;} \llbracket true \rrbracket) \cup (\llbracket true \rrbracket \mathbin{;} \llbracket P \rrbracket) \cup (\llbracket P \rrbracket \mathbin{;} \llbracket true \rrbracket) \cup \llbracket P \rrbracket,$$

which would include all possibilities, it is more convenient to make the equivalent but more succinct definition

$$\llbracket \Diamond P \rrbracket \mathrel{\widehat{=}} \overline{\llbracket true \rrbracket} \mathbin{;} \llbracket P \rrbracket \mathbin{;} \overline{\llbracket true \rrbracket}.$$

We also define $\llbracket \Box P \rrbracket \mathrel{\widehat{=}} \mathbb{I} \setminus \llbracket \Diamond \neg P \rrbracket$.

Note that $\llbracket \Box P \rrbracket$ is not necessarily the same as $\llbracket P \rrbracket$: while $\llbracket \delta = 1 \rrbracket$ is the set of all intervals of length one, $\llbracket \Box \delta = 1 \rrbracket$ is the empty set, as every interval has a subinterval of length less than one. However, $\llbracket \Box P \rrbracket = \llbracket P \rrbracket$ if whenever P holds on an interval, it holds on every subinterval also [11].

We illustrate concatenation with the following example. Suppose that if the water level in a mine has been above the danger level for at least *Delay* time units, then the mine pump must be switched on. This is expressed by

$$\llbracket H_2O > DangerH_2O \;\wedge\; \delta \geq Delay \rrbracket \subseteq \overline{\llbracket true \rrbracket} \mathbin{;} \llbracket Pump = On \rrbracket.$$

Note that the unspecified brackets permit the join to be either open-closed or closed-open concatenation.

2.4 Laws

In Figure 1 we present a selection of laws applicable to reasoning about the above specification notation, in addition to the usual laws of set theory. Law 13 is an existing law, but its proof differs from that in the Duration Calculus. This is because endpoints of intervals are fixed in DC, with the result that there is an upper bound on the number of alternations of P and $\neg P$ in the interval. On the other hand, endpoints are arbitrary in TIC, so there is no upper bound on the number of alternations. For this reason, there are restrictions on H which do not exist in DC. For example, $H(X) \mathrel{\widehat{=}} \neg(\overline{\mathbb{I}} \subseteq X)$ satisfies all conditions in Law 13 except that it contains negation, and fails the conclusion. The law is proved in Appendix A.

Laws 14 to 18 are new, with proofs in Appendix B, while the others are analogous to laws in the Duration Calculus [3, 9]. In Figure 1, P, Q and R are predicates that may contain, unless otherwise stated, free occurrences of α, ω and δ. Also, S, T, U and V are sets of time intervals, i.e. they are of type $\mathbb{P}\,\mathbb{I}$.

The induction law on trace histories, Law 14, will form the basis of the proof in the mine pump case study. The induction law on interval lengths, Law 13, will not be used in the mine pump case study. The main difference between the two laws is that instead of the induction being over intervals with arbitrary starting point, the intervals have starting point $\alpha < 0$ since $\llbracket \omega < 0 \Rightarrow \alpha < 0 \rrbracket = \llbracket \mathit{true} \rrbracket$.

Law 15 will be important in the mine pump example, where $\{I\}$ will represent an arbitrary history of the property $S \subseteq T$ which we wish to prove. This arbitrary history will be constructed by induction (Law 14). Note that the law would not hold if we replaced $\{I\}$ by an arbitrary set $U \subseteq \llbracket \alpha < r \rrbracket$: for example, $\llbracket \alpha < 0 \rrbracket \mathbin{;} \llbracket \alpha = 1 \wedge \omega = 3 \rrbracket \subseteq \llbracket \alpha < 0 \rrbracket \mathbin{;} \llbracket \alpha = 2 \wedge \omega = 3 \rrbracket$ because both sides equal $\llbracket \alpha < 0 \wedge \omega = 3 \rrbracket$, but $\llbracket \alpha = 1 \wedge \omega = 3 \rrbracket \not\subseteq \llbracket \alpha = 2 \wedge \omega = 3 \rrbracket$.

The *finite variability property* is defined to hold for a property P if there exists duration $\xi > 0$ such that $\llbracket \neg P \rrbracket \mathbin{;} \llbracket \Diamond P \rrbracket \mathbin{;} \llbracket \neg P \rrbracket \subseteq \llbracket \delta \geq \xi \rrbracket$. In Law 17, this property is not necessary for closed right endpoints. For open right endpoints, define predicate $Q : \mathbb{T}^3 \rightarrow \mathbb{B}$ by $Q(t, \alpha, \omega) \mathrel{\widehat{=}} t \in \mathbb{Q}$, where $\mathbb{Q}$ is the set of rational numbers. Then

$$\llbracket \mathit{true} \rrparenthesis \neq \varnothing = \overline{\llbracket \mathit{true} \rrbracket} \mathbin{;} \varnothing = \overline{\llbracket \mathit{true} \rrbracket} \mathbin{;} (\llbracket Q \rrparenthesis \cup \llbracket \neg Q \rrparenthesis).$$

3 Application: A Mine Pump

Consider the case of a mine [1], where miners work in a confined space and there is danger of mine collapse, flooding and the accumulation of gases. Here, the operation of the mine is considered only as it relates to the level of water in the mine. A pump operates to remove water from the mine if the water reaches a certain level, but only if the concentration of methane in the mine is sufficiently low to permit the safe operation of the pump: a high level of methane combined with a spark from the pump may result in an explosion. Our aim will be to prove that the water level in the mine will not be at a level which prevents mining too long or too often. This will be done using the property that the level of

Law 1 (Monotonicity) *If for all* α, ω *and* δ *in* $\mathbb{T}$ *and all* $t : (\alpha \ldots \omega]$ $P(t, \alpha, \omega) \;\Rightarrow\; Q(t, \alpha, \omega)$, *then* $(\!-P-\!] \;\subseteq\; (\!-Q-\!]$.

Law 2 (True and false) $\llbracket true \rrbracket \;=\; \mathbb{I}$ *and* $\llbracket false \rrbracket \;=\; \varnothing$.

Law 3 (And) $\llbracket P \rrbracket \cap \llbracket Q \rrbracket \;=\; \llbracket P \wedge Q \rrbracket$.

Law 4 (Or) $\llbracket P \rrbracket \cup \llbracket Q \rrbracket \;\subseteq\; \llbracket P \vee Q \rrbracket$.

Law 5 (Not) $\llbracket \neg\, P \rrbracket \;\subseteq\; \mathbb{I} \setminus \llbracket P \rrbracket$.

Law 6 (Concatenation monotonicity) *If* $S \subseteq S'$ *and* $T \subseteq T'$, *then* $S\,;T \;\subseteq\; S'\,;T'$.

Law 7 (Concatenation associativity) $(S\,;T)\,;U \;=\; S\,;(T\,;U)$.

Law 8 (Concatenation zero and unit) $S\,;\varnothing = \varnothing\,;S = \varnothing$ *and* $S\,;\mathbf{1} = \mathbf{1}\,;S = S$.

Law 9 (Concatenate union) $(S \cup T)\,;U \;=\; (S\,;U) \cup (T\,;U)$ *and* $S\,;(T \cup U) \;=\; (S\,;T) \cup (S\,;U)$.

Law 10 (Concatenate intersection) $(S \cap T)\,;U \;\subseteq\; (S\,;U) \cap (T\,;U)$ *and* $U\,;(S \cap T) \;\subseteq\; (U\,;S) \cap (U\,;T)$. *Equality holds in the first case if* ω *and* δ *are not free in* S *and* T, *and in the second case if* α *and* δ *are not free in* S *and* T.

Law 11 (Concatenate property) *If* α, ω *and* δ *do not occur free in* P, *then* $\llbracket P \wedge \delta > 0 \rrbracket \;=\; \llbracket P \rrbracket\,;\llbracket P \rrbracket$.

Law 12 (Always) *If* α, ω *and* δ *are not free in* P, *then* $\llbracket \Box P \rrbracket \;=\; \llbracket P \rrbracket$.

Law 13 (Induction on Lengths) *Let* $H(X)$ *be a formula containing* $X : \mathbb{P}\,\mathbb{I} \cup \{\mathbf{1}\}$, *but no occurrence of negation or the complement of* X. *Let* P *be a predicate for which the finite variability property holds. If*

- $H(\mathbf{1})$ *and*
- $H(X) \Rightarrow H(X \cup (X\,;\llbracket P \rrbracket) \cup (X\,;\llbracket \neg P \rrbracket))$

then $H(\overline{\mathbb{I}})$.

Law 14 (Induction on Histories) *Let* $H(X)$ *be a formula containing* $X : \mathbb{P}\,\mathbb{I}$, *but no occurrence of negation or the complement of* X. *Let* P *be a predicate for which the finite variability property holds. If*

- $H(\llbracket \omega < 0 \rrbracket)$ *and*
- $H(X) \Rightarrow H(X \cup (X\,;\llbracket P \rrbracket) \cup (X\,;\llbracket \neg P \rrbracket))$

then $H(\llbracket \alpha < 0 \rrbracket)$.

Law 15 (Ignore Prefix) *Suppose that there exists* $r : \mathbb{T}$ *such that for all* $I : \llbracket \alpha < r \rrbracket$, $\{I\}\,;S \subseteq \{I\}\,;T$. *Then* $S \subseteq T$.

Law 16 (Distribute Intersection) *If* α, ω *and* δ *are not free in* P, *then* $\llbracket P \rrbracket \cap (S\,;T) = (\llbracket P \rrbracket \cap S)\,;(\llbracket P \rrbracket \cap T)$.

Law 17 (Endpoints) *If* α, ω *and* δ *are not free in* P *and* Q, *and if* P *or* Q *is finitely variable, then* $\llbracket P \vee Q \rrbracket \;=\; \overline{\llbracket P \vee Q \rrbracket}\,;(\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \;=\; (\llbracket P \rrbracket \cup \llbracket Q \rrbracket)\,;\overline{\llbracket P \vee Q \rrbracket}$.

Law 18 (Implicit Duration) *If* α, ω *and* δ *are not free in* P *and* Q, *then* $\llbracket P \wedge \delta \geq r \rrbracket \subseteq \overline{\llbracket true \rrbracket}\,;\llbracket Q \rrbracket \Leftrightarrow \llbracket P \wedge \delta \geq r \rrbracket \subseteq \overline{\llbracket \delta \leq r \rrbracket}\,;\llbracket Q \rrbracket$.

Figure 1: Laws for manipulating timed traces.

methane is not high too long or too often, permitting the timely operation of the mine pump.

3.1 Specification: The Environment

The levels of water and methane in the mine are represented by the continuous functions $H_2O : \mathbb{T} \rightarrow \mathbb{R}$ and $CH_4 : \mathbb{T} \rightarrow \mathbb{R}$ respectively. The methane level below which the mine pump may be switched on safely, if required, is $HighCH_4$, and the water level above which it is desirable to switch the mine pump on is $HighH_2O$. We wish to prevent the water level from reaching the dangerous level $DangerH_2O$, where $DangerH_2O > HighH_2O$, whenever possible. We make the abbreviations

$$\begin{array}{rcl} HCH_4 & \widehat{=} & CH_4 \geq HighCH_4 \\ HH_2O & \widehat{=} & H_2O \geq HighH_2O \\ DH_2O & \widehat{=} & H_2O \geq DangerH_2O. \end{array}$$

Note that $DH_2O \Rightarrow HH_2O$.

We need some assumptions on the environment, without which we cannot prove the desired property. Specifically, these are the initial conditions of the system, the constraints on the frequency and duration of high methane levels, and a constraint on the rate of inflow of water into the mine. We require that initially, the water level of the system is low. Otherwise, there may not be enough time for the pump to be switched on before the water level becomes dangerous, so that the condition on the frequency or the duration of dangerous water levels may be violated. We begin to observe the system at time 0, so we stipulate that up to and including time 0, the water level is low:

$$[\![\omega \leq 0]\!] \quad \subseteq \quad [\![\neg HH_2O]\!]. \tag{1}$$

The rate of inflow of water into the mine is constrained to be at most $MaxInflow$:

$$\mathbb{I} \quad = \quad [\![H_2O(\omega) - H_2O(\alpha) \leq MaxInflow.\delta]\!]. \tag{2}$$

This will prevent the water from rising to the dangerous level too quickly, thus allowing sufficient time for the pump to switch on. The top of Figure 2 depicts a possible variation of the water level, with this condition restricting the gradient of the water level. Note that the condition allows for the possibility of the water level falling, even when the mine pump is off; this is reflected in the oscillation of the water level around $DangerH_2O$.

The duration and frequency of high methane levels directly determine when the pump is prevented from being turned on, so the constraints on them must be specified. The methane level may not be high for more than E time units at once, while any two periods of high methane levels must be separated by at least ξ time units:

$$\begin{array}{rcll} [\![HCH_4]\!] & \subseteq & [\![\delta \leq E]\!] & (3) \\ [\![HCH_4]\!] \, ; [\![\neg HCH_4]\!] \, ; [\![HCH_4]\!] & \subseteq & [\![\delta \geq \xi]\!]. & (4) \end{array}$$

Section 3.3 will place constraints on E and ξ.

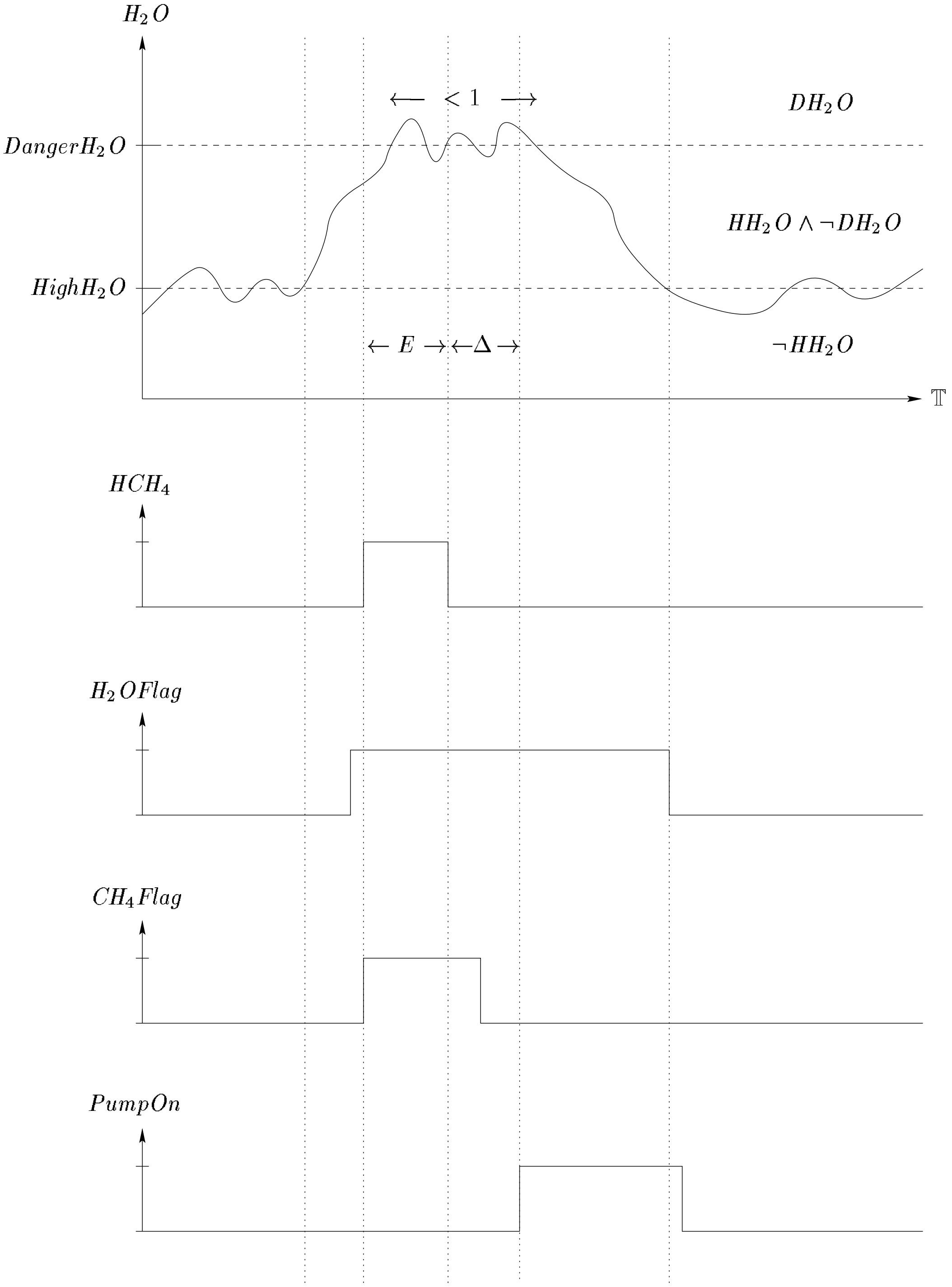
H_2O
$\longleftarrow \;<1\; \longrightarrow$
DH_2O
$DangerH_2O$
$HH_2O \wedge \neg DH_2O$
$HighH_2O$
$\leftarrow E \rightarrow \leftarrow \Delta \rightarrow$
$\neg HH_2O$
$\mathbb{T}$
HCH_4
H_2OFlag
CH_4Flag
$PumpOn$

Figure 2: A possible mine pump behaviour.

3.2 Specification: The Desired Property

We will show that periods of dangerous water levels are either within one time unit of each other, or they are far apart. In the former case, the water level may be continually dangerous, or interspersed with times when the water level is not dangerous. This reflects the possibility that the water level oscillates around the dangerous level when the pump has not yet been switched on (see Figure 2). Formally, the condition which we wish to prove is

$$\lceil DH_2O\rceil \,;\, \lceil \delta \geq 1\rceil \,;\, \lceil DH_2O\rceil \quad \subseteq \quad \lceil \delta \geq \xi - \Delta - 1\rceil, \tag{5}$$

where Δ (and ξ) will be constrained in Section 3.3. This condition literally states that if two periods of dangerous water levels are separated by at least one time unit, then they must be separated by at least $\xi - \Delta - 1$ time units. Therefore in Figure 2, less than one time unit separates the time when the water level first reaches $DangerH_2O$ and the time the water level last drops below $DangerH_2O$.

While the condition would be satisfied by a long time period for which the water level is continually dangerous, such a long time period will have a subperiod for which the condition fails.

The proof of the condition will rely on an implementation of the mine pump which ensures that the mine pump is switched on when the water level is high, but before the water level has had time to rise to dangerous, provided that the methane level is sufficiently low to allow safe operation of the pump.

3.3 Implementation: The Pump

The mine pump operates to remove water from the mine if the water reaches a high level ($HighH_2O$), but only if the level of methane in the mine is sufficiently low to permit the safe operation of the pump: a high level of methane combined with a spark from the pump may result in an explosion.

The levels of water and methane are measured by sensors, and reaction-time delays may occur between a high level occurring and the mine pump registering this high level. High levels of water and methane have been registered when flags $H_2OFlag : \mathbb{T} \to \mathbb{B}$ and $CH_4Flag : \mathbb{T} \to \mathbb{B}$ respectively have been set. The delays are no more than $DelayH_2O$ time units in the case of the water sensor and $DelayCH_4$ time units in the case of the methane sensor. These delay constraints are expressed in our notation as:

$$\lceil HH_2O \wedge \delta \geq DelayH_2O\rceil \quad \subseteq \quad \overline{\lceil true\rceil} \,;\, \lceil H_2OFlag\rceil \tag{6}$$

$$\lceil \neg HCH_4 \wedge \delta \geq DelayCH_4\rceil \quad \subseteq \quad \overline{\lceil true\rceil} \,;\, \lceil \neg CH_4Flag\rceil. \tag{7}$$

Thus, if the water level is high for at least $DelayH_2O$ time units, the flag H_2OFlag must be set after at most $DelayH_2O$ time units. A similar consideration applies to the methane level.

Once the appropriate flags have been set for the operation of the mine pump, a further delay may occur before the mine pump starts. This is expressed by

$$\lceil H_2OFlag \wedge \neg CH_4Flag \wedge \delta \geq DelayPump\rceil \quad \subseteq \quad \overline{\lceil true\rceil} \,;\, \lceil PumpOn\rceil, \tag{8}$$

where $\mathit{PumpOn} : \mathbb{T} \to \mathbb{B}$ holds if the mine pump is operating, and $\mathit{DelayPump}$ is the delay between the appropriate flags being set and the mine pump being switched on.

Appendix C shows that conditions 6 to 8 can be combined to yield

$$\lceil\!\lceil HH_2O \wedge \neg HCH_4 \wedge \delta \geq \Delta \rceil\!\rceil \quad \subseteq \quad \overline{\lceil\!\lceil \delta \leq \Delta \rceil\!\rceil} \,;\, \lceil\!\lceil \mathit{PumpOn} \rceil\!\rceil, \tag{9}$$

where

$$\Delta \quad \widehat{=} \quad max(\mathit{DelayCH}_4, \mathit{DelayH}_2O) + \mathit{DelayPump}.$$

We now state some constraints on the operation of the mine pump, which will facilitate the proof later. We constrain the delay in the operation of the pump as follows:

$$E + \Delta \quad < \quad \frac{\mathit{DangerH}_2O - \mathit{HighH}_2O}{\mathit{MaxInflow}}. \tag{10}$$

Thus, the delay in the operation of the pump (resulting from high methane levels and sensor delays) can be no higher than the minimum time taken for the water level to rise from HighH_2O to $\mathit{DangerH}_2O$.

Once the mine pump has been switched on, the level of water in the mine decreases at a rate of at least $\mathit{MinOutflow} > 0$; this is expressed in our notation as follows:

$$\lceil\!\lceil \mathit{PumpOn} \rceil\!\rceil \quad \subseteq \quad \lceil\!\lceil H_2O(\omega) - H_2O(\alpha) \leq -\mathit{MinOutflow}.\delta \rceil\!\rceil. \tag{11}$$

The constraint

$$E + \Delta \quad \leq \quad \frac{1}{1 + \frac{\mathit{MaxInflow}}{\mathit{MinOutflow}}} \tag{12}$$

ensures that $\mathit{MinOutflow}$ is large enough to limit the period where the water level is dangerous to one time unit, thereby compensating for both the maximum rate $\mathit{MaxInflow}$ of water and the delay $E + \Delta$ in switching the mine pump on. The constraint

$$\xi \quad > \quad 1 + 2\Delta + \frac{\mathit{DangerH}_2O - \mathit{HighH}_2O}{\mathit{MinOutflow}} \tag{13}$$

ensures that the gap ξ between dangerous methane concentrations is large enough to compensate for the time required to reduce the water level from dangerous to low.

It is reasonable to constrain the mine pump's operation so that it is switched off if the water level is sufficiently low or the methane level is high. Otherwise, the property that the water level is not too high too often could be satisfied easily by leaving the pump on permanently. This trivial solution can be ruled out (perhaps because the pump might be damaged by running dry) by imposing conditions on the mine pump's operation:

$$\begin{array}{rcl}
\llbracket \neg HH_2O \wedge \delta \geq DelayH_2O \rrbracket & \subseteq & \overline{\llbracket true \rrbracket} \,;\, \llbracket \neg H_2OFlag \rrbracket \\
\llbracket HCH_4 \wedge \delta \geq DelayCH_4 \rrbracket & \subseteq & \overline{\llbracket true \rrbracket} \,;\, \llbracket CH_4Flag \rrbracket \\
\llbracket (\neg H_2OFlag \vee CH_4Flag) \wedge \delta \geq DelayPump \rrbracket & \subseteq & \overline{\llbracket true \rrbracket} \,;\, \llbracket \neg PumpOn \rrbracket .
\end{array}$$

These conditions are analogous to conditions 6 to 8, except that they relate to the mine pump being switched off rather than on. We will not use these conditions in our proof: by ignoring them, we implicitly assume the worst case that the mine pump is off unless conditions 6 to 8 result in the pump being on. This shows that there is no disadvantage in underspecification.

3.4 Proof: Induction Law

We show that conditions 1 to 4 on the environment and conditions 6 to 13 on the mine pump imply the goal condition 5. Central to the proof is the idea that before any period when the water level is dangerous (i.e. DH_2O holds), there must have been a period when the water level was low (i.e. $\neg HH_2O$ held). As a result, the time taken for the water level to rise from low to dangerous gives the pump sufficient time to switch itself on and restrict the period of time when the water level is dangerous. This suggests that a proof using induction on the history of the water level is required.

Thus, it suffices to show that for all intervals $I : \llbracket \alpha < 0 \rrbracket$,

$$\{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket \quad \subseteq \quad \{I\} \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \qquad (14)$$

since then Law 15 can be applied to achieve the desired result. Law 14 is an induction law on histories rather than interval lengths, so it seems like a suitable law to use. The most obvious induction hypothesis is

$$\begin{array}{rcl}
H(X) & \widehat{=} & \forall I : X \;\; \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket \\
 & & \qquad\qquad \subseteq \{I\} \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket
\end{array}$$

as then the conclusion of the induction law corresponds to condition 14.

However, it turns out that this proposed induction hypothesis is not strong enough, and that it is necessary to incorporate the consideration that before any period when the water level is dangerous, it must have been low previously. The strengthened induction hypothesis is

$$\begin{array}{rcl}
H(X) & \widehat{=} & \forall I : X \;\; \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket \\
 & & \qquad \subseteq \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket \\
 & & \wedge X \,;\, \llbracket HH_2O \rrbracket \subseteq \overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HH_2O \rrbracket \,;\, \llbracket HH_2O \rrbracket .
\end{array}$$

Note that the first conjunct of the induction hypothesis is stronger than the required conclusion; this facilitates the proof of the induction step for the first conjunct with $I : X \,;\, \llbracket DH_2O \rrbracket$.

The application of the induction law on trace histories (Law 14) could occur with $P \mathrel{\widehat{=}} DH_2O$ or $P \mathrel{\widehat{=}} \neg HH_2O$, but we choose the latter as the resulting proof is slightly simpler. The finite variability property necessary for the application of the induction law does not follow from the specification or from the continuity of H_2O. However we assume the finite variability property here, as it seems like a reasonable property to hold in the physical world, being a constraint on how rapidly the water level can oscillate.

Note that high methane levels and high water levels do not necessarily coincide: while a high water level must be preceded by a high methane level, there may or may not be overlap. Each case must be considered, and for this reason, the proof is intrinsically non-trivial. However, motivation for the proof strategy will be provided wherever possible, and steps are presented in detail for completeness. The proof relies largely on the lemmas to be proven in the next section. The monotonicity law (Law 6) is used so often that instances of its use will not be mentioned.

For the first conjunct of the base step, with $I : \llbracket \omega < 0 \rrbracket$,

$$\begin{array}{ll}
 & \{I\} \mathbin{;} \llbracket DH_2O \rrbracket \mathbin{;} \llbracket \delta \geq 1 \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{condition 1} \\
 & \llbracket \neg HH_2O \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket \mathbin{;} \llbracket \delta \geq 1 \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket \\
= & \hfill \text{continuity of } H_2O \text{ (see Section 3.1)} \\
 & \varnothing \\
\subseteq & \\
 & \{I\} \mathbin{;} \llbracket DH_2O \rrbracket \mathbin{;} \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket.
\end{array}$$

For the second conjunct of the base step,

$$\begin{array}{ll}
 & \llbracket \omega < 0 \rrbracket \mathbin{;} \llbracket HH_2O \rrbracket \\
\subseteq & \hfill \text{condition 1} \\
 & \llbracket \neg HH_2O \rrbracket \mathbin{;} \llbracket HH_2O \rrbracket \\
\subseteq & \hfill \text{definition of } \mathbf{1} \text{ and Law 9} \\
 & \overline{\llbracket true \rrbracket} \mathbin{;} \llbracket \neg HH_2O \rrbracket \mathbin{;} \llbracket HH_2O \rrbracket.
\end{array}$$

For the first conjunct of the induction step, let

$$I : X \cup (X \mathbin{;} \llbracket \neg HH_2O \rrbracket) \cup (X \mathbin{;} \llbracket HH_2O \rrbracket).$$

If $I : X$, then

$$\begin{array}{ll}
 & \{I\} \mathbin{;} \llbracket DH_2O \rrbracket \mathbin{;} \llbracket \delta \geq 1 \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket \\
\subseteq & \{I\} \mathbin{;} \llbracket DH_2O \rrbracket \mathbin{;} \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \mathbin{;} \llbracket DH_2O \rrbracket
\end{array}$$

follows immediately from the induction hypothesis. If $I : X \mathbin{;} \llbracket \neg HH_2O \rrbracket$, then there exist $I_1 : X$ and $I_2 : \llbracket \neg HH_2O \rrbracket$ such that $\{I\} = \{I_1\} \mathbin{;} \{I_2\}$ and

$$\begin{array}{lr}
\quad \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
= & \\
\quad \{I_1\} ; \{I_2\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
\subseteq & I_2 : \llbracket \neg HH_2O \rrbracket \\
\quad \{I_1\} ; \llbracket \neg HH_2O \rrbracket ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
= & \text{continuity of } H_2O \\
\quad \varnothing & \\
\subseteq & \\
\quad \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq \xi - \Delta - 1 \rrbracket ; \llbracket DH_2O \rrbracket . &
\end{array}$$

If $I : X ; \llbracket HH_2O \rrbracket$, then from the induction hypothesis there exists $I_1 : \overline{\llbracket true \rrbracket}$ and $I_2 : \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket$ such that $\{I\} = \{I_1\} ; \{I_2\}$ and

$$\begin{array}{lr}
\quad \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
= & \\
\quad \{I_1\} ; \{I_2\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
\subseteq & \text{Theorem 1 below} \\
\quad \{I_1\} ; \{I_2\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq \xi - \Delta - 1 \rrbracket ; \llbracket DH_2O \rrbracket & \\
= & \\
\quad \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq \xi - \Delta - 1 \rrbracket ; \llbracket DH_2O \rrbracket . &
\end{array}$$

The second conjunct of the induction step is shown by

$$\begin{array}{lr}
\quad (X \cup (X ; \llbracket \neg HH_2O \rrbracket) \cup (X ; \llbracket HH_2O \rrbracket)) ; \llbracket HH_2O \rrbracket & \\
\subseteq & \text{Law 9} \\
\quad (X ; \llbracket HH_2O \rrbracket) \cup (X ; \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket) & \\
\subseteq & \text{induction hypothesis} \\
\quad (\overline{\llbracket true \rrbracket} ; \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket) \cup (X ; \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket) & \\
\subseteq & X \subseteq \overline{\llbracket true \rrbracket} \\
\quad \overline{\llbracket true \rrbracket} ; \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket . &
\end{array}$$

This completes the main part of the proof. Note that the proof uses only one condition explicitly, 1; the other conditions are used in proving the lemmas of the next section.

The following theorem corresponds to a single step in the proof above.

Theorem 1 *For all* $I : \llbracket \neg HH_2O \rrbracket ; \llbracket HH_2O \rrbracket$,

$$\begin{array}{rl}
& \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \rrbracket ; \llbracket DH_2O \rrbracket \\
\subseteq & \{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq \xi - \Delta - 1 \rrbracket ; \llbracket DH_2O \rrbracket
\end{array}$$

Proof: Figure 2 suggests that the separation of periods of dangerous water levels depends on whether or not the water level is low in between: if it is low in between, then we aim to show that the separation is at least $\xi - \Delta - 1$. On the other hand, if the water level is not low in between, then we aim to show that the separation cannot be 1 or more. These two cases are covered by Lemmas 1 and 2 in the next section, and depend on the separation of periods of high methane levels (condition 13) to permit the timely operation of the pump. Formally, let $I : \llbracket \neg HH_2O \rrbracket \,;\, \llbracket HH_2O \rrbracket$. Then

$$
\begin{array}{ll}
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket \\
= & \hfill \text{By definition of } \Box \text{ and Law 12, } \llbracket HH_2O \rrbracket \cup \llbracket \Diamond \neg HH_2O \rrbracket = \mathbb{I} \\
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, (\llbracket \delta \geq 1 \rrbracket \cap (\llbracket HH_2O \rrbracket \cup \llbracket \Diamond \neg HH_2O \rrbracket)) \,;\, \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{Laws 9 and 3} \\
 & (\{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \wedge HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket) \\
 & \cup(\{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \Diamond \neg HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket) \\
\subseteq & \hfill \text{Lemmas 1 and 2} \\
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket. \qquad \Box
\end{array}
$$

3.5 Proof: Lemmas

In this section, we prove the results necessary in the application of the induction law in the previous section. The first two lemmas correspond to the two cases in Theorem 1, while Lemma 3 is a technical lemma used in their proof.

The first lemma states that two times when the water level is dangerous cannot be separated by a period of length one or more where the water level is high continually.

Lemma 1 *For all* $I : \llbracket \neg HH_2O \rrbracket \,;\, \llbracket HH_2O \rrbracket$,

$$\{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq 1 \wedge HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket \;=\; \varnothing.$$

Proof: First we sketch the proof informally. Assume that two times when the water level is dangerous are separated by a period of length one or more where the water level is high continually. Then, by Lemma 3, the methane level must have been high at most Δ time units before the first time when the water level was dangerous. As a result, the pump must be switched on at most $E + \Delta$ time units after the water level first became dangerous. There are two cases to consider: first, the pump remains on until the last time the water level is dangerous, which is ruled out because this would mean that the pump has been on sufficiently long for the water level to drop below dangerous. In the second case, the pump is switched off before the last time the water level is dangerous because of high methane levels, but has been on sufficiently long for the water level to drop below high. This is also a contradiction.

Formally, first consider the special case where $I : \llbracket \neg HH_2O \rrbracket ; \llbracket \neg DH_2O \wedge HH_2O \rrbracket$. Then there exist $I_1 : \llbracket \neg HH_2O \rrbracket$ and $I_2 : \llbracket \neg DH_2O \wedge HH_2O \rrbracket$ such that $\{I\} = \{I_1\} ; \{I_2\}$ and

$$\{I\} ; \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket$$

$$\subseteq \qquad \text{Lemma 3}$$

$$\begin{array}{l} \{I_1\} ; (\{I_2\} \cap (\llbracket \mathit{true} \rrbracket ; \llbracket HCH_4 \rrbracket ; \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})); \\ \llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket \end{array}$$

$$\subseteq \qquad \text{condition 3}$$

$$\begin{array}{l} \{I_1\} ; (\{I_2\} \cap (\llbracket \mathit{true} \rrbracket ; \llbracket HCH_4 \rrbracket ; \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})); \\ \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \\ \cap(\overline{\llbracket HCH_4 \wedge \delta \leq E \rrbracket} ; \llbracket \neg HCH_4 \rrbracket ; \overline{\llbracket \mathit{true} \rrbracket})\Big) \end{array}$$

$$\subseteq \qquad \text{conditions 4 and 12}$$

$$\begin{array}{l} \{I_1\} ; (\{I_2\} \cap (\llbracket \mathit{true} \rrbracket ; \llbracket HCH_4 \rrbracket ; \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})); \\ \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \cap \Big(\overline{\llbracket HCH_4 \wedge \delta \leq E \rrbracket}; \\ ((\llbracket \neg HCH_4 \wedge \delta \geq \xi - \Delta \rrbracket ; \overline{\llbracket \mathit{true} \rrbracket}) \cup \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket)\Big)\Big) \end{array}$$

$$\subseteq$$

$$\begin{array}{l} \{I_1\} ; \{I_2\}; \\ \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \\ \cap(\overline{\llbracket \delta \leq E \rrbracket} ; ((\llbracket \neg HCH_4 \wedge \delta \geq \xi - \Delta \rrbracket ; \overline{\llbracket \mathit{true} \rrbracket}) \cup \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket))\Big) \end{array}$$

$$\subseteq \qquad \text{condition 9 and Law 16}$$

$$\begin{array}{l} \{I_1\} ; \{I_2\}; \\ \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \\ \cap(\overline{\llbracket \delta \leq E \rrbracket} ; \overline{\llbracket \delta < \Delta \rrbracket} ; ((\llbracket \mathit{PumpOn} \wedge \delta \geq \xi - 2\Delta \rrbracket ; \overline{\llbracket \mathit{true} \rrbracket}) \cup \llbracket \mathit{PumpOn} \rrbracket))\Big) \end{array}$$

$$\subseteq \qquad \text{condition 2}$$

$$\begin{array}{l} \{I\} ; \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \cap \Big(\overline{\llbracket \delta < E + \Delta \rrbracket}; \\ ((\llbracket \mathit{PumpOn} \wedge \delta \geq \xi - 2\Delta \wedge H_2O(\alpha) \leq \mathit{DangerH_2O} + (E + \Delta).\mathit{MaxInflow} \rrbracket; \\ \overline{\llbracket \mathit{true} \rrbracket}) \cup \llbracket \mathit{PumpOn} \wedge H_2O(\alpha) \leq \mathit{DangerH_2O} + (E + \Delta).\mathit{MaxInflow} \rrbracket)\Big)\Big) \end{array}$$

$$\subseteq \qquad \text{condition 11}$$

$$\begin{array}{l} \{I\} ; \Big((\llbracket DH_2O \rrbracket ; \llbracket \delta \geq 1 \wedge HH_2O \rrbracket ; \llbracket DH_2O \rrbracket) \cap \Big(\overline{\llbracket \delta < E + \Delta \rrbracket}; \\ ((\llbracket \mathit{PumpOn} \wedge \delta \geq \xi - 2\Delta \wedge \mathit{HighH_2O} \leq H_2O(\omega) \leq \mathit{DangerH_2O} \\ \quad +(E + \Delta).\mathit{MaxInflow} - \mathit{MinOutflow}.\delta \rrbracket ; \overline{\llbracket \mathit{true} \rrbracket}) \\ \cup \llbracket \mathit{PumpOn} \wedge \mathit{DangerH_2O} \leq H_2O(\omega) \leq \mathit{DangerH_2O} \\ \quad +(E + \Delta).\mathit{MaxInflow} - \mathit{MinOutflow}.\delta \rrbracket)\Big)\Big) \end{array}$$

$$\subseteq$$

$$\begin{aligned}&\{I\}\,;\Big(\llbracket\delta \geq 1\rrbracket \cap \Big(\overline{\llbracket\delta < E + \Delta\rrbracket};\\&((\llbracket\delta \geq \xi - 2\Delta \wedge \delta \leq \tfrac{DangerH_2O - HighH_2O + (E+\Delta).MaxInflow}{MinOutflow}\rrbracket\,;\,\overline{\llbracket true\rrbracket})\\&\cup\llbracket\delta \leq \tfrac{(E+\Delta).MaxInflow}{MinOutflow}\rrbracket)\Big)\Big)\end{aligned}$$

$$\subseteq$$

$$\begin{aligned}&\{I\}\,;\Big(\llbracket\delta \geq 1\rrbracket\cap\\&(\llbracket\Diamond(\delta \geq \xi - 2\Delta \wedge \delta \leq \tfrac{DangerH_2O - HighH_2O + (E+\Delta).MaxInflow}{MinOutflow})\rrbracket\\&\cup\llbracket\delta < (E + \Delta).(1 + \tfrac{MaxInflow}{MinOutflow})\rrbracket)\Big)\end{aligned}$$

$$\subseteq \qquad\qquad \text{condition 12}$$

$$\{I\}\,;(\llbracket\delta \geq 1\rrbracket \cap (\llbracket\Diamond(\delta \geq \xi - 2\Delta \wedge \delta < 1 + \tfrac{DangerH_2O - HighH_2O}{MinOutflow})\rrbracket \cup \llbracket\delta < 1\rrbracket))$$

$$\subseteq \qquad\qquad \text{condition 13}$$

$$\{I\}\,;(\llbracket\delta \geq 1\rrbracket \cap (\llbracket\Diamond false\rrbracket \cup \llbracket\delta < 1\rrbracket))$$

$$=$$

$$\varnothing.$$

Now consider the general case where $I : \llbracket\neg HH_2O\rrbracket\,;\,\llbracket HH_2O\rrbracket$. From the continuity of H_2O, there exist $I_1 : \llbracket\neg HH_2O\rrbracket\,;\,\llbracket\neg DH_2O \wedge HH_2O\rrbracket$ and $I_2 : \llbracket DH_2O\rrbracket\,;\,\llbracket HH_2O\rrbracket$ such that $\{I\} = \{I_1\}\,;\{I_2\}$. So

$$\{I\}\,;\llbracket DH_2O\rrbracket\,;\llbracket\delta \geq 1 \wedge HH_2O\rrbracket\,;\llbracket DH_2O\rrbracket$$

$$=$$

$$\{I_1\}\,;\{I_2\}\,;\llbracket DH_2O\rrbracket\,;\llbracket\delta \geq 1 \wedge HH_2O\rrbracket\,;\llbracket DH_2O\rrbracket$$

$$\subseteq$$

$$\{I_1\}\,;\llbracket DH_2O\rrbracket\,;\llbracket\delta \geq 1 \wedge HH_2O\rrbracket\,;\llbracket DH_2O\rrbracket$$

$$= \qquad\qquad \text{special case above and Law 8}$$

$$\varnothing. \qquad \Box$$

The second lemma states that if the water level is low between two periods when the water level is dangerous, then the two periods must be separated by at least $\xi - \Delta - 1$ time units.

Lemma 2 *For all* $I : \llbracket\neg HH_2O\rrbracket\,;\,\llbracket HH_2O\rrbracket$,

$$\begin{aligned}&\{I\}\,;\llbracket DH_2O\rrbracket\,;\llbracket\Diamond\neg HH_2O\rrbracket\,;\llbracket DH_2O\rrbracket\\ \subseteq\;&\{I\}\,;\llbracket DH_2O\rrbracket\,;\llbracket\delta \geq \xi - \Delta - 1\rrbracket\,;\llbracket DH_2O\rrbracket\end{aligned}$$

Proof: First we sketch the proof informally. By Lemma 3, both periods of dangerous water levels must have been preceded (within Δ time units) by periods of high methane. By condition 13, these periods of high methane must be separated by at least ξ time units. The resulting arithmetic leaves $\xi - \Delta - 1$ time units between periods of dangerous water levels.

Formally, let $I : \llbracket \neg HH_2O \rrbracket \,;\, \llbracket HH_2O \rrbracket$. Then there exist $I_1 : \llbracket \neg HH_2O \rrbracket$, $I_2 : \llbracket \neg DH_2O \wedge HH_2O \rrbracket$ and $I_3 : \overline{\llbracket DH_2O \rrbracket \,;\, \llbracket HH_2O \rrbracket}$ such that $\{I\} = \{I_1\} ; \{I_2\} ; \{I_3\}$ and

$$
\begin{array}{ll}
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \Diamond \neg HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{definition of } \llbracket \Diamond \neg HH_2O \rrbracket \text{ and continuity of } H_2O \\
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket true \rrbracket \,;\, \llbracket \neg HH_2O \rrbracket \,;\, \llbracket \neg DH_2O \wedge HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket ; \\
 & \overline{\llbracket HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket} \\
\subseteq & \hfill \text{Lemma 3} \\
 & \{I_1\} \,;\, (\{I_2\} \cap (\llbracket true \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})) \,;\, \{I_3\} ; \\
 & \llbracket DH_2O \rrbracket \,;\, \llbracket true \rrbracket \,;\, \llbracket \neg HH_2O \rrbracket \,;\, \llbracket \neg DH_2O \wedge HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket ; \\
 & \overline{\llbracket HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket} \\
\subseteq & \hfill \text{Lemma 3} \\
 & \{I_1\} \,;\, (\{I_2\} \cap (\llbracket true \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})) \,;\, \{I_3\} ; \\
 & \llbracket DH_2O \rrbracket \,;\, \llbracket true \rrbracket \,;\, \llbracket \neg HH_2O \rrbracket \,;\, \Big(\llbracket \neg DH_2O \wedge HH_2O \rrbracket \\
 & \cap (\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket true \rrbracket}) \Big) \,;\, \llbracket DH_2O \rrbracket \,;\, \overline{\llbracket HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket} \\
\subseteq & \hfill \text{Lemma 1} \\
 & \{I_1\} \,;\, (\{I_2\} \cap (\llbracket true \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})) \,;\, \Big((\{I_3\} ; \\
 & \llbracket DH_2O \rrbracket) \cap \llbracket \delta < 1 \rrbracket \Big) \,;\, \llbracket true \rrbracket \,;\, \Big(\llbracket \neg DH_2O \wedge HH_2O \rrbracket \\
 & \cap (\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket true \rrbracket}) \Big) \,;\, \llbracket DH_2O \rrbracket \,;\, \overline{\llbracket HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket} \\
\subseteq & \hfill \text{condition 4} \\
 & \{I_1\} \,;\, (\{I_2\} \cap (\llbracket true \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})) \,;\, \Big((\{I_3\} ; \\
 & \llbracket DH_2O \rrbracket) \cap \llbracket \delta < 1 \rrbracket \Big) \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \,;\, \Big(\llbracket \neg DH_2O \wedge HH_2O \rrbracket \\
 & \cap (\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket true \rrbracket}) \Big) \,;\, \llbracket DH_2O \rrbracket \,;\, \overline{\llbracket HH_2O \rrbracket \,;\, \llbracket DH_2O \rrbracket} \\
\subseteq & \\
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \,;\, \llbracket \delta \geq \xi - \Delta - 1 \rrbracket \,;\, \llbracket DH_2O \rrbracket . \qquad \Box
\end{array}
$$

We prove these results using the following lemma, which states that if the water reaches a dangerous level, the methane level must have been high within Δ time units previously.

Lemma 3 *Let* $I : \llbracket \neg HH_2O \rrbracket \,;\, \llbracket \neg DH_2O \wedge HH_2O \rrbracket$, $I_1 : \llbracket \neg HH_2O \rrbracket$ *and* $I_2 : \llbracket \neg DH_2O \wedge HH_2O \rrbracket$ *such that* $\{I\} = \{I_1\} ; \{I_2\}$. *Then*

$$
\begin{array}{ll}
 & \{I\} \,;\, \llbracket DH_2O \rrbracket \\
\subseteq & \{I_1\} \,;\, (\{I_2\} \cap (\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket})) \,;\, \llbracket DH_2O \rrbracket
\end{array}
$$

Proof: All intervals can be characterised in the following way:

$$
\begin{array}{ll}
& \mathbb{I} \\
= & \hfill \text{Laws 17 and 9; finite variability follows from condition 4} \\
& (\overline{\llbracket true \rrbracket} \,;\, \llbracket HCH_4 \rrbracket) \cup (\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \rrbracket) \\
= & \hfill \text{Law 9} \\
& (\overline{\llbracket true \rrbracket} \,;\, \llbracket HCH_4 \rrbracket) \cup (\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket) \\
& \cup(\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket) \\
= & \hfill \text{Laws 17 and 9} \\
& (\overline{\llbracket true \rrbracket} \,;\, \llbracket HCH_4 \rrbracket) \cup (\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket) \\
& \cup(\overline{\llbracket true \rrbracket} \,;\, \llbracket HCH_4 \rrbracket \,;\, \llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket) \cup \llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket \\
\subseteq & \\
& (\overline{\llbracket true \rrbracket} \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket}) \\
& \cup(\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket) \cup \llbracket \delta < \Delta \rrbracket \\
\subseteq & \hfill \text{definition of } \Box \text{ and Law 12} \\
& (\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket}) \\
& \cup(\llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket}) \\
& \cup(\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket) \cup \llbracket \delta < \Delta \rrbracket.
\end{array}
$$

The proof strategy is to apply Law 9 to $\{I_1\};(\{I_2\}\cap\mathbb{I});\llbracket DH_2O \rrbracket$, with the above characterisation of $\mathbb{I}$, and show that the term corresponding to $\llbracket \Diamond \neg HCH_4 \rrbracket \,;\, \llbracket HCH_4 \rrbracket \,;\, \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket}$ is the only one which is not empty.

If the methane level has been low and the water level has been high for sufficiently long, then the pump must have been switched on, with the result that the water level is being reduced:

$$
\begin{array}{ll}
& \{I_1\} \,;\, (\{I_2\} \cap (\overline{\llbracket true \rrbracket} \,;\, \llbracket \neg HCH_4 \wedge \delta \geq \Delta \rrbracket)) \,;\, \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{condition 9} \\
& \{I_1\} \,;\, (\{I_2\} \cap (\overline{\llbracket true \rrbracket} \,;\, \llbracket PumpOn \rrbracket)) \,;\, \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{condition 11} \\
& \{I_1\} \,;\, \Big(\{I_2\} \\
& \cap(\overline{\llbracket true \rrbracket} \,;\, \llbracket PumpOn \wedge H_2O(\omega) \leq H_2O(\alpha) < DangerH_2O \rrbracket)\Big) \,; \\
& \llbracket DH_2O \wedge H_2O(\alpha) \geq DangerH_2O \rrbracket \\
= & \hfill \text{continuity of } H_2O \text{ and Law 8} \\
& \varnothing.
\end{array}
$$

The maximum rate of water inflow prevents the water level from rising from $HighH_2O$ to $DangerH_2O$ in too short an interval:

$$
\begin{array}{ll}
& \{I_1\} \mathbin{;} (\{I_2\} \cap ((\llbracket HCH_4 \rrbracket \mathbin{;} \overline{\llbracket \neg HCH_4 \wedge \delta < \Delta \rrbracket}) \cup \llbracket \delta < \Delta \rrbracket)) \mathbin{;} \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{condition 3} \\
& \{I_1\} \mathbin{;} (\{I_2\} \cap ((\llbracket \delta \leq E \rrbracket \mathbin{;} \overline{\llbracket \delta < \Delta \rrbracket}) \cup \llbracket \delta < \Delta \rrbracket)) \mathbin{;} \llbracket DH_2O \rrbracket \\
= & \\
& \{I_1\} \mathbin{;} (\{I_2\} \cap \llbracket \delta < E + \Delta \rrbracket) \mathbin{;} \llbracket DH_2O \rrbracket \\
\subseteq & \hfill \text{continuity of } H_2O \text{ and condition 2} \\
& \{I_1\} \mathbin{;} \Big(\{I_2\} \cap \llbracket \delta < E + \Delta \wedge H_2O(\alpha) = HighH_2O \wedge H_2O(\omega) < HighH_2O \\
& +MaxInflow.(E + \Delta) \rrbracket \Big) \mathbin{;} \llbracket DH_2O \wedge H_2O(\alpha) \geq DangerH_2O \rrbracket \\
= & \hfill \text{condition 10; continuity of } H_2O \\
& \varnothing .
\end{array}
$$

Applying the proof strategy mentioned previously to $\{I_1\} \mathbin{;} (\{I_2\} \cap \mathbb{I}) \mathbin{;} \llbracket DH_2O \rrbracket$ yields the desired result. □

4 Conclusion

We have presented the set-theoretic Timed Interval Calculus, and demonstrated its use in specification and reasoning about the mine pump case study. We have introduced new concepts and transformation laws to this end. In particular, the induction law on trace histories was the basis of the verification of the safety property. This verification is difficult, which raises the practical issue of whether or not one would attempt such a proof if faced with the budget and time constraints of industrial verification. While tool support would aid in the verification, the particular challenge in this case study was designing the proof strategy, a problem which a tool does not help with.

Many real-world computer systems will be at least as complex as the mine pump case study, and this is a challenge which must be faced. We believe that the verification proof in the case study is intrinsically complex, given the different timing combinations of high water and methane levels which must be considered. For this reason, substantial case studies such as the mine pump offer valuable guidance to programmers about to tackle similar challenges.

Acknowledgements

I gratefully acknowledge the many helpful comments of Karl Lermer, Colin Fidge and Graeme Smith. This research was funded by the Information Technology Division of the Defence Science and Technology Organisation.

References

[1] A. Burns and A.J. Wellings. *Real-Time Systems and their Programming Languages.* Addison-Wesley, 1989.

[2] C.J. Fidge, I.J. Hayes, A.P. Martin and A.K. Wabenhorst. A Set-Theoretic Model for Real-Time Specification and Reasoning. In J. Jeuring (Ed) *Mathematics of Program Construction (MPC'98)*, Lecture Notes in Computer Science Vol. 1422, pages 188–206, Springer-Verlag, 1998.

[3] M. R. Hansen and Zhou Chaochen. Duration calculus: Logical foundations. *Formal Aspects of Computing*, 9(3):283–330, 1997.

[4] B. von Karger. A Proof Rule for Control Loops. In J. Jeuring (Ed) *Mathematics of Program Construction (MPC'98)*, Lecture Notes in Computer Science Vol. 1422, pages 7–22, Springer-Verlag, 1998.

[5] Z.M. Liu. Specification and Verification in the Duration Calculus. In M. Joseph (Ed) *Real-Time Systems—Specification, Verification and Analysis*, pages 182–228, Springer-Verlag, 1996.

[6] B. P. Mahony and I. J. Hayes. A case-study in timed refinement: A mine pump. *IEEE Transactions on Software Engineering*, 18(9):817–826, 1992.

[7] B. Moszkowski. *Executing Temporal Logic Programs.* Cambridge University Press, 1986.

[8] E.-R. Olderog, A. P. Ravn, and J. U. Skakkebæk. Refining system requirements to program specifications. In C. Heitmeyer and D. Mandrioli, editors, *Formal Methods for Real-Time Computing*, volume 5 of *Trends in Software*, chapter 5, pages 107–134. Wiley, 1996.

[9] A. P. Ravn. *Design of Embedded Real-Time Computing Systems.* PhD thesis, Department of Computer Science, Technical University of Denmark, 1995.

[10] D. Scholefield, H. Zedan, and He Jifeng. A specification-oriented semantics for the refinement of real-time systems. *Theoretical Computer Science*, 131:219–241, 1994.

[11] Zhou Chaochen, C.A.R. Hoare and A.P. Ravn. A Calculus of Durations. *Information Processing Letters*, 40:269–276, 1991.

[12] Zhou Chaochen. Duration calculi: An overview. In D. Bjørner, M. Broy, and I. Pottosin, editors, *Formal Methods in Programming and Their Applications*, volume 735 of *Lecture Notes in Computer Science*, pages 256–266. Springer-Verlag, 1993. Extended abstract.

A Proof of Law 13

Let $H(X)$ be a formula containing $X : \mathbb{PI} \cup \{\mathbf{1}\}$, but no occurrence of negation or the complement of X. More precisely, define formula $H(X)$ in terms of *expressions* as follows. For arbitrary sets of intervals S^k, expressions $E(X)$, $E_1(X)$ and $E_2(X)$ are defined by

$$E(X) \;\widehat{=}\; X \mid S^k \mid E_1(X) \cup E_2(X) \mid E_1(X) \cap E_2(X) \mid E_1(X) \,;\, E_2(X)$$

and formulae $H(X)$, $H_1(X)$ and $H_2(X)$ are defined by

$$\begin{aligned} H(X) \quad &\widehat{=} \quad E_1(X) \subseteq E_2(X) \mid \forall\, I \in X \;\, H_1(X) \mid H_1(X) \wedge H_2(X) \\ &\qquad \mid H_1(X) \vee H_2(X). \end{aligned}$$

Note that $E_1(X) = E_2(X)$ is equivalent to $E_1(X) \subseteq E_2(X) \;\wedge\; E_2(X) \subseteq E_1(X)$. For predicate P which satisfies the finite variability property, define

$$\begin{aligned} X_0 \quad &\widehat{=} \quad \mathbf{1} \\ X_{i+1} \quad &\widehat{=} \quad X_i \cup (X_i \,;\, \llbracket P \rrbracket) \cup (X_i \,;\, \llbracket \neg P \rrbracket). \end{aligned}$$

Thus, we have $H(X_0)$ and $H(X_i) \Rightarrow H(X_{i+1})$ for all $i \in \mathbb{N}$, and so by induction $H(X_i)$ for all $i \in \mathbb{N}$. From the finite variability property for P, $\overline{\mathbb{I}} = \bigcup_{i \in \mathbb{N}} X_i$. The proof is the same as that in DC, and will not be shown here.

We have seen that $\forall\, i \in \mathbb{N} \;\, H(X_i)$, and that $\overline{\mathbb{I}} = \bigcup_{i \in \mathbb{N}} X_i$, so that $H(\overline{\mathbb{I}}) = H(\bigcup_{i \in \mathbb{N}} X_i)$. Thus to prove that $H(\overline{\mathbb{I}})$, it suffices to show that

$$(\forall\, i \in \mathbb{N} \;\, H(X_i)) \Rightarrow H(\textstyle\bigcup_{i \in \mathbb{N}} X_i).$$

The following two lemmas are proven first.

Lemma 4 *If $E(X)$ is an expression and $i < j$, then $E(X_i) \subseteq E(X_j)$.*

Proof: The proof is by induction on the construction of $E(X)$. For the case where $E(X) = X$, $X_i \subseteq X_j$ by the definition of X_i and X_j. For $E(X) = S^k$, where X does not occur in S^k, the result is trivial. For $E(X) = E_1(X) \cup E_2(X)$,

$$\begin{aligned} &\quad E(X_i) \\ = & \qquad\qquad\qquad\qquad \text{definition of } E(X_i) \\ &\quad E_1(X_i) \cup E_2(X_i) \\ \subseteq & \qquad\qquad\qquad\qquad \text{induction hypothesis} \\ &\quad E_1(X_j) \cup E_2(X_j) \\ = & \qquad\qquad\qquad\qquad \text{definition of } E(X_j) \\ &\quad E(X_j). \end{aligned}$$

The proof for $E(X) = E_1(X) \cap E_2(X)$ is exactly the same, except that $\cap$ replaces $\cup$ in the proof. The proof for $E(X) = E_1(X) \,;\, E_2(X)$ is also the same, except that ; replaces $\cup$, and the step which uses the induction hypothesis also requires the use of Law 6. □

Lemma 5 *For any expression $E(X)$, $E(\bigcup_{i\in\mathbb{N}} X_i) = \bigcup_{i\in\mathbb{N}} E(X_i)$.*

Proof: The proof is by induction on the construction of $E(X)$. The cases where $E(X) = X$ and $E(X) = S^k$ (X not occurring in S^k) are entirely trivial. For the case where $E(X) = E_1(X) \cup E_2(X)$,

$$\begin{array}{ll}
& E(\bigcup_{i\in\mathbb{N}} X_i) \\
= & \hfill \text{definition of } E(\bigcup_{i\in\mathbb{N}} X_i) \\
& E_1(\bigcup_{i\in\mathbb{N}} X_i) \cup E_2(\bigcup_{i\in\mathbb{N}} X_i) \\
= & \hfill \text{induction hypothesis} \\
& (\bigcup_{i\in\mathbb{N}} E_1(X_i)) \cup (\bigcup_{i\in\mathbb{N}} E_2(X_i)) \\
= & \\
& \bigcup_{i\in\mathbb{N}}(E_1(X_i) \cup E_2(X_i)) \\
= & \hfill \text{definition of } E(X_i) \\
& \bigcup_{i\in\mathbb{N}} E(X_i).
\end{array}$$

For the case where $E(X) = E_1(X) \cap E_2(X)$,

$$\begin{array}{ll}
& E(\bigcup_{i\in\mathbb{N}} X_i) \\
= & \hfill \text{definition of } E(\bigcup_{i\in\mathbb{N}} X_i) \\
& E_1(\bigcup_{i\in\mathbb{N}} X_i) \cap E_2(\bigcup_{i\in\mathbb{N}} X_i) \\
= & \hfill \text{induction hypothesis} \\
& (\bigcup_{i\in\mathbb{N}} E_1(X_i)) \cap (\bigcup_{i\in\mathbb{N}} E_2(X_i)) \\
= & \\
& \bigcup_{i\in\mathbb{N}} \bigcup_{j\in\mathbb{N}}(E_1(X_i) \cap E_2(X_j)) \\
= & \hfill \text{the } \supseteq \text{ direction is trivial; for } \subseteq\text{, use Lemma 4} \\
& \bigcup_{i\in\mathbb{N}}(E_1(X_i) \cap E_2(X_i)) \\
= & \hfill \text{definition of } E(X_i) \\
& \bigcup_{i\in\mathbb{N}} E(X_i).
\end{array}$$

The proof for $E(X) = E_1(X) ; E_2(X)$ is the same as for $E(X) = E_1(X) \cap E_2(X)$, except that ; replaces $\cup$. In addition, the third of the five proof steps requires the generalisation of Law 9 to infinite unions, and the fourth of the five proof steps also requires the use of Law 6. □

The result which we wish to show, namely $(\forall\, i \in \mathbb{N}\ H(X_i)) \Rightarrow H(\bigcup_{i\in\mathbb{N}} X_i)$, follows from Theorem 2.

Theorem 2 *For a formula $H(X)$ not containing negation or the complement of X, $(\forall\, i \in \mathbb{N}\ \exists j \geq i\ H(X_j)) \Rightarrow H(\bigcup_{i\in\mathbb{N}} X_i)$.*

Proof: The proof is by induction on the construction of $H(X)$. For the case where $H(X) \Leftrightarrow E_1(X) \subseteq E_2(X)$,

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ H(X_j)$$

$\Leftrightarrow$ definition of $H(X_j)$

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ E_1(X_j) \subseteq E_2(X_j)$$

$\Rightarrow$ Lemma 4

$$(\bigcup_{j\in\mathbb{N}} E_1(X_j)) \subseteq (\bigcup_{j\in\mathbb{N}} E_2(X_j))$$

$\Leftrightarrow$ Lemma 5

$$E_1(\bigcup_{j\in\mathbb{N}} X_j) \subseteq E_2(\bigcup_{j\in\mathbb{N}} X_j)$$

$\Leftrightarrow$ definition of $H(\bigcup_{j\in\mathbb{N}} X_j)$

$$H(\bigcup_{j\in\mathbb{N}} X_j).$$

For the case where $H(X) \Leftrightarrow \forall\, I \in X\ \ H_1(X)$,

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ H(X_j)$$

$\Leftrightarrow$ definition of $H(X_j)$

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ \forall\, I \in X\ \ H_1(X_j)$$

$\Rightarrow$

$$\forall\, I \in X\ \ \forall\, i \in \mathbb{N}\ \exists j \geq i\ H_1(X_j)$$

$\Rightarrow$ induction hypothesis

$$\forall\, I \in X\ \ H_1(\bigcup_{i\in\mathbb{N}} X_i)$$

$\Leftrightarrow$ definition of $H(\bigcup_{i\in\mathbb{N}} X_i)$

$$H(\bigcup_{i\in\mathbb{N}} X_i).$$

For the case where $H(X) \Leftrightarrow (H_1(X) \wedge H_2(X))$,

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ H(X_j)$$

$\Leftrightarrow$ definition of $H(X_j)$

$$\forall\, i \in \mathbb{N}\ \exists j \geq i\ (H_1(X_j) \wedge H_2(X_j))$$

$\Rightarrow$

$$(\forall\, i \in \mathbb{N}\ \exists j \geq i\ H_1(X_j)) \wedge (\forall\, i \in \mathbb{N}\ \exists j \geq i\ H_2(X_j))$$

$\Rightarrow$ induction hypothesis

$$H_1(\bigcup_{i\in\mathbb{N}} X_i) \wedge H_2(\bigcup_{i\in\mathbb{N}} X_i)$$

$\Leftrightarrow$ definition of $H(\bigcup_{i\in\mathbb{N}} X_i)$

$$H(\bigcup_{i\in\mathbb{N}} X_i).$$

For $H(X) \Leftrightarrow (H_1(X) \vee H_2(X))$, the proof is exactly the same as for $H(X) \Leftrightarrow (H_1(X) \wedge H_2(X))$, except that $\wedge$ is replaced by $\vee$. □

B Proofs of New Laws

Proof:[Law 14]
Define $H'(X) \mathrel{\widehat{=}} H(\llbracket \omega < 0 \rrbracket \mathbin{;} X)$, and apply Law 13 to $H'(X)$. The base case follows immediately from $H'(\mathbf{1}) \Leftrightarrow H(\llbracket \omega < 0 \rrbracket)$. For the step case,

$$H'(X)$$

$\Leftrightarrow$ definition of $H'(X)$

$$H(\llbracket \omega < 0 \rrbracket \mathbin{;} X)$$

$\Rightarrow$ induction step for H

$$H((\llbracket \omega < 0 \rrbracket \mathbin{;} X) \cup (\llbracket \omega < 0 \rrbracket \mathbin{;} X \mathbin{;} \llbracket P \rrbracket) \cup (\llbracket \omega < 0 \rrbracket \mathbin{;} X \mathbin{;} \llbracket \neg P \rrbracket))$$

$\Leftrightarrow$ Law 9

$$H(\llbracket \omega < 0 \rrbracket \mathbin{;} (X \cup (X \mathbin{;} \llbracket P \rrbracket) \cup (X \mathbin{;} \llbracket \neg P \rrbracket)))$$

$\Leftrightarrow$ definition of H'

$$H'(X \cup (X \mathbin{;} \llbracket P \rrbracket) \cup (X \mathbin{;} \llbracket \neg P \rrbracket)).$$

From Law 13, $H'(\overline{\mathbb{I}})$. So $H(\llbracket \omega < 0 \rrbracket \mathbin{;} \overline{\mathbb{I}})$. Since $\llbracket \omega < 0 \rrbracket \mathbin{;} \overline{\mathbb{I}} = \llbracket \alpha < 0 \rrbracket$, we have $H(\llbracket \alpha < 0 \rrbracket)$. □

Proof:[Law 15]
Suppose that there exists $r : \mathbb{T}$ such that for all $I : \llbracket \alpha < r \rrbracket$, $\{I\} \mathbin{;} S \subseteq \{I\} \mathbin{;} T$. Let $I' : S$. Choose $I : \llbracket \alpha < r \rrbracket$ such that $\{I\};\{I'\} \neq \varnothing$. Since $\{I\};\{I'\} \subseteq \{I\};S$, $\{I\} \mathbin{;} \{I'\} \subseteq \{I\} \mathbin{;} T$. Since $\{I\} \mathbin{;} \{I'\} \neq \varnothing$, $I' : T$. □

Proof:[Law 16]
Suppose α, ω and δ are not free in P, and let $I : \mathbb{I}$. Then

$$I \in \llbracket P \rrbracket \cap (S \mathbin{;} T)$$

$\Leftrightarrow$

$$I \in \llbracket P \rrbracket \wedge \exists\, J \in S \;\; \exists\, J' \in T \;\; \{I\} = \{J\} \mathbin{;} \{J'\}$$

$\Leftrightarrow$ α, ω and δ are not free in P

$$\exists\, J \in \llbracket P \rrbracket \cap S \;\; \exists\, J' \in \llbracket P \rrbracket \cap T \;\; \{I\} = \{J\} \mathbin{;} \{J'\}$$

$\Leftrightarrow$

$$I \in (\llbracket P \rrbracket \cap S) \mathbin{;} (\llbracket P \rrbracket \cap T)$$

□

Proof:[Law 17]
First we show

$$\llbracket P \vee Q \rrbracket = (\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}.$$

For $\supseteq$ in this equality,

$$(\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}$$

$$\subseteq \qquad \text{Laws 1 and 6}$$

$$\llbracket P \vee Q \rrbracket \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}$$

$$\subseteq \qquad \text{Law 11}$$

$$\llbracket P \vee Q \rrbracket$$

For $\subseteq$ in the equality, we use Law 13 with

$$H(X) \mathrel{\widehat{=}} X \cap \llbracket P \vee Q \rrbracket \subseteq (\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}.$$

For the base case, clearly $H(\mathbf{1})$ holds because $\mathbf{1} \cap \llbracket P \vee Q \rrbracket = \varnothing$. For the step case,

$$(X \cup (X \mathbin{;} \llbracket P \rrbracket) \cup (X \mathbin{;} \llbracket \neg P \rrbracket)) \cap \llbracket P \vee Q \rrbracket$$

$$\subseteq \qquad \text{set theory}$$

$$(X \cap \llbracket P \vee Q \rrbracket) \cup ((X \mathbin{;} \llbracket P \rrbracket) \cap \llbracket P \vee Q \rrbracket) \cup ((X \mathbin{;} \llbracket \neg P \rrbracket) \cap \llbracket P \vee Q \rrbracket)$$

$$\subseteq \qquad \text{Laws 16, 3 and 1}$$

$$(X \cap \llbracket P \vee Q \rrbracket) \cup ((X \cap \llbracket P \vee Q \rrbracket) \mathbin{;} \llbracket P \rrbracket) \cup ((X \cap \llbracket P \vee Q \rrbracket) \mathbin{;} \llbracket Q \rrbracket)$$

$$\subseteq \qquad \text{induction hypothesis and Law 6}$$

$$((\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}) \cup ((\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket} \mathbin{;} \llbracket P \rrbracket)$$
$$\cup ((\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket} \mathbin{;} \llbracket Q \rrbracket)$$

$$\subseteq \qquad \text{Laws 1 and 6}$$

$$((\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}) \cup ((\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket} \mathbin{;} \llbracket P \vee Q \rrbracket)$$

$$\subseteq \qquad \text{Law 11}$$

$$(\llbracket P \rrbracket \cup \llbracket Q \rrbracket) \mathbin{;} \overline{\llbracket P \vee Q \rrbracket}$$

The proof that

$$\llbracket P \vee Q \rrbracket = \overline{\llbracket P \vee Q \rrbracket} \mathbin{;} (\llbracket P \rrbracket \cup \llbracket Q \rrbracket)$$

is very similar, but uses a variation of Law 13 with

$$H(X) \Rightarrow H(X \cup (\llbracket P \rrbracket \mathbin{;} X) \cup (\llbracket \neg P \rrbracket \mathbin{;} X))$$

as the proof obligation for the step case. □

Proof:[Law 18]
The $\Leftarrow$ direction follows from $\llbracket \delta \leq r \rrbracket \subseteq \llbracket true \rrbracket$ and monotonicity (Law 6).

For the $\Rightarrow$ direction, let $I \in \llbracket P \wedge \delta \geq r \rrbracket$. Consider first the case where $\sup I - \inf I = r$. By hypothesis, $I = I_1 \cup I_2$, where $I_1 \in \overline{\llbracket true \rrbracket}$ and $I_2 \in \llbracket Q \rrbracket$, and where for all $t_1 \in I_1$ and all $t_2 \in I_2$, $t_1 < t_2$. Since $\sup I - \inf I = r$ and $I_1 \subseteq I$, $\sup I_1 - \inf I_1 \leq r$. So $I_1 \in \overline{\llbracket \delta \leq r \rrbracket}$ and $I \in \overline{\llbracket \delta \leq r \rrbracket} \mathbin{;} \llbracket Q \rrbracket$.

The case where $\sup I - \inf I > r$ remains to be considered. In this case, there exist $I_1 \in \llbracket \delta = r \rrbracket$ and $I_2 \in \llbracket true \rrbracket$ such that $I = I_1 \cup I_2$ and for all $t_1 \in I_1$

and all $t_2 \in I_2$, $t_1 < t_2$. Since $I_1 \in \overline{\llbracket \delta \leq r \rrbracket}$, it suffices to show that $I_2 \in \llbracket Q \rrbracket$. Since α, ω and δ are not free in Q, it suffices to show that for all $t \in I_2$, $Q(t)$. So choose any $t \in I_2$, and let I_3 be the prefix of I_2 with right closed endpoint t. Then

$$true$$

$\Leftrightarrow$

$$I \in \llbracket P \wedge \delta \geq r \rrbracket$$

$\Leftrightarrow$ $\qquad I = I_1 \cup I_2$

$$I_1 \cup I_2 \in \llbracket P \wedge \delta \geq r \rrbracket$$

$\Rightarrow$ $\qquad I_1 \in \llbracket \delta = r \rrbracket$; I_3 is a prefix of I_2; and α, ω and δ are not free in P

$$I_1 \cup I_3 \in \llbracket P \wedge \delta \geq r \rrbracket$$

$\Rightarrow$ $\qquad$ hypothesis

$$I_1 \cup I_3 \in \overline{\llbracket true \rrbracket} \,;\, \llbracket Q \rrbracket$$

$\Rightarrow$ $\qquad I_3$ has right closed endpoint t

$$Q(t).$$

□

C Proof of condition 9

$$\llbracket HH_2O \wedge \neg HCH_4 \wedge \delta \geq \Delta \rrbracket$$

$\subseteq$ $\qquad$ definition of Δ

$$\llbracket \delta \geq \Delta \rrbracket \cap \llbracket HH_2O \wedge \delta \geq DelayH_2O \rrbracket \cap \llbracket \neg HCH_4 \wedge \delta \geq DelayCH_4 \rrbracket$$

$\subseteq$ $\qquad$ conditions 6, 7 and Law 18

$$\llbracket \delta \geq \Delta \rrbracket \cap (\overline{\llbracket \delta \leq DelayH_2O \rrbracket} \,;\, \llbracket H_2OFlag \rrbracket) \cap (\overline{\llbracket \delta \leq DelayCH_4 \rrbracket} \,;\, \llbracket \neg CH_4Flag \rrbracket)$$

$\subseteq$ $\qquad$ Law 10

$$\llbracket \delta \geq \Delta \rrbracket \cap (\overline{\llbracket \delta \leq max(DelayH_2O, CH_4Flag) \rrbracket} \,;\, \llbracket H_2OFlag \wedge \neg CH_4Flag \rrbracket)$$

$\subseteq$ $\qquad$ definition of Δ

$$\overline{\llbracket \delta \leq max(DelayH_2O, CH_4Flag) \rrbracket} \,;\, \llbracket H_2OFlag \wedge \neg CH_4Flag \wedge \delta \geq DelayPump \rrbracket$$

$\subseteq$ $\qquad$ condition 8 and Law 18

$$\overline{\llbracket \delta \leq max(DelayH_2O, CH_4Flag) \rrbracket} \,;\, \overline{\llbracket \delta \leq DelayPump \rrbracket} \,;\, \llbracket PumpOn \rrbracket$$

$\subseteq$ $\qquad$ definition of Δ

$$\overline{\llbracket \delta \leq \Delta \rrbracket} \,;\, \llbracket PumpOn \rrbracket \qquad \square$$