A theory for execution-time derivation in real-time programs

Karl Lermer\textsuperscript{a}, Colin J. Fidge\textsuperscript{b}, Ian J. Hayes\textsuperscript{a,} \textsuperscript{*}

\textsuperscript{a}School of Information Technology and Electrical Engineering, The University of Queensland, Queensland 4072, Australia
\textsuperscript{b}School of Software Engineering and Data Communications, Queensland University of Technology, Queensland 4001, Australia

Abstract

We provide an abstract command language for real-time programs and outline how a partial correctness semantics can be used to compute execution times. The notions of a timed command, refinement of a timed command, the command traversal condition, and the worst-case and best-case execution time of a command are formally introduced and investigated with the help of an underlying weakest liberal precondition semantics. The central result is a theory for the computation of worst-case and best-case execution times from the underlying semantics based on supremum and infimum calculations. The framework is applied to the analysis of a message transmitter program and its implementation.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Real-time programming; Control-flow analysis; Execution-time derivation and prediction; Predicate transformer semantics; Partial correctness

1. Introduction

State-of-the-art development of safety-critical systems must guarantee the implementation of the system’s safety requirements to the highest possible assurance level. This especially applies to real-time systems where producing results between certain time bounds is crucial for correct and safe behaviour. The major advances in real-time programming have been in the areas of scheduling periodic processes [5,6] and worst-case
execution-time analysis of program code [8,23]. Together these allow the design of systems as a set of communicating processes, where each process consists of a block of code which is repeatedly executed with a given (fixed) period. In order to successfully schedule such a set of processes it is necessary to know the worst-case execution time of the block of code associated with each process.

The requirements of a reactive real-time system are most succinctly specified in terms of a relation between inputs and outputs over all time. To bridge the gap between such high-level system requirements and real-time implementations that satisfy those requirements, a theory of real-time software development is required [20]. Fig. 1 shows our approach to formal development and timing analysis of real-time systems. This figure outlines the development of a real-time system from an abstract specification into a high-level language program to a machine-code implementation in a specific environment. The separation of timing behaviour and functional behaviour [13] is a key feature of this framework that allows a more abstract approach to the program development process. Real-time program development is partitioned into

- a machine-independent phase that, given the specification of a real-time system, develops a machine-independent program, annotated with timing requirements, to meet the specification [14,20], and
- a machine-dependent phase, that checks that the compiled version of the program will meet all its timing requirements when it is executed on the particular target machine [24,25].

This partitioning makes it possible to perform abstract reasoning about timing requirements in the system design and high-level language program, and to separately prove that the requirements are satisfied by the compiled code.

Within this framework, timing analysis begins by annotating the program with the programmer’s real-time requirements. This can be done by extending the program semantics with a variable to denote the current time [21] and by adding a “deadline” statement to the programming language [13] which allows bounds on the current time to be expressed.
We have also developed methods to derive sequential real-time programs from specifications [20] and perform timing analysis [15]. This paper focuses on using the program’s semantics to derive execution times for real-time programs. In particular, we are interested in high-level program analysis where the derivation of execution times for annotated real-time programs is essential for the formulation of timing constraints. These constraints can be used in the subsequent timing analysis phase to verify that the compiled machine code has acceptable timing behaviour. This phase refers to the dashed ellipses in Fig. 1. Numerous algorithms and tools for predicting worst-case execution times from both high-level and machine-level code already exist [35,34,28,11]. Our goal here is not to derive yet another such algorithm, but to elaborate the semantic theory that underlies these implementations. We investigate the notions of timed commands and their associated execution times from a fundamental perspective, and thus provide a sound theoretical basis for the justification of the correctness of execution-time analysis techniques.

The remainder of this paper is structured as follows. Section 2 states the syntax and semantics for abstract commands. The notions of command and timed command are defined. Section 3 defines the entry and traversal conditions for commands. Section 4 defines the liberal refinement relation on the command language. In Section 5, the notions of worst-case and best-case execution times are introduced for timed commands. As a main result, we present a method for symbolic computation of traversal conditions, and worst-case and best-case execution times. In Section 6 these techniques are applied to a “message transmitter” example. Three appendices at the end of the paper contain important definitions and theorems.

1.1. Related work

In this paper, we develop a semantic theory for deriving traversal conditions for, and execution-time expressions from, real-time program paths. Both of these goals have been explored previously, but from a pragmatic, rather than theoretical, perspective. Extraction and analysis of “program paths”, or “partial programs”, has long been a cornerstone of static program analysis [22]. For efficiency and ease of use, the aim is usually to devise algorithms that can be applied automatically and syntactically to a program or program path.

Path traversal conditions are important because they can be used to show that programmer-supplied assertions are consistent with the code, and that the code itself is internally consistent. For instance, Bergeretti and Carré devised algorithms that manipulate matrices representing information flow between the statements in a path in order to analyse programs for coding errors such as ineffective assignments [4]. Subsequently, a data-flow analysis algorithm was incorporated in the SPADE program analysis tool [7] and its successors. In particular, the SPARK Examiner tool uses weakest precondition semantics for program paths [3]. A particularly explicit tool for path traversal condition calculation is the Path Exploration Tool [16]. It allows the programmer to select a control-flow path through a program and a simple algorithm then calculates the path’s traversal condition. A particularly important application of algorithms that calculate path traversal conditions is to identify “dead”, or “infeasible”, program paths, i.e., those that can never be followed at run time [7,8]. In previous work, we described a semantic basis for such dead path analysis [18].
Analysing program paths to predict their worst-case (and sometimes best-case) execution times is a standard requirement of high-integrity real-time programming. The process is awkward because the actual execution time of the final system cannot be known until the program is compiled and the particular host processor and operating environment are chosen. The most accurate timing predictions are those made by analysing paths through the compiled assembler code [36], although even this is difficult for code that will run on pipelined and cached processors [28]. However, our interest here is also with high-level language program analysis. In this case, the program is divided into its individual control-flow paths and formulas corresponding to each language construct in the path can be used to derive an execution-time expression for that path. The resulting expression may be symbolic, or it may be instantiated with specific execution times for each primitive component to produce a numerical result [35, 33]. For instance, Chapman et al. present practical algorithms for partitioning high-level language programs into paths, eliminating dead paths by calculating their traversal conditions, and predicting the worst-case execution times of the remainder based on a cost function associated with each path component [8]. (Eliminating dead paths is particularly important in static timing analysis, because incorporating their execution times can severely distort the overall timing predictions [12, 27].) Puschner and Schell’s approach to timing analysis uses graph theory to extract paths which are then assessed using a worst-case execution-time function [34]. Engblom and Ermedahl convert control-flow information to linear constraints to support subsequent execution-time analysis [11]. Park advocates an approach in which the programmer uses an explicit ‘path language’ to identify those paths to be analysed for their worst-case execution times [32].

Whichever technique is used, to be effective in practice, automatic algorithms for identifying path traversal conditions and predicting worst-case execution times must work syntactically because they cannot afford the overheads of semantic theorem proving. Our goal below, therefore, is to provide the general semantics underlying such algorithms, thus providing a sound basis for justifying their correctness.

2. Syntax and semantics for timed commands

This section presents a general language for real-time programs on the basis of a partial correctness semantics. For some real-time programs their correct behaviour for some inputs may be to never terminate, for example, a loop waiting for an external signal will never terminate if the signal never arrives. Additionally, there are situations in which the signal may only appear transiently: in these cases, the loop may or may not detect the signal and hence may or may not terminate; either behaviour is correct in this situation.

We would like to reason about the timing behaviour of such programs, for example, if the loop in the above example detects the signal and terminates, it may be required to respond to the signal within some deadline. For this reason, weakest liberal precondition (\(wl\)p) semantics [10] are used in this paper. Recall that \(wl\)p\((S, R)\) is the weakest predicate characterising initial states from which predicate \(R\) is guaranteed to hold in the final state, provided that command \(S\) terminates. This can be contrasted with weakest precondition (\(wp\)) semantics in which \(wp\)(\(S, R\)) characterises those initial states from which \(S\) is both guaranteed to terminate and establish \(R\) on termination. The following relationship holds
between wp and wlp:

\[ wp(S, R) \equiv wp(S, true) \land wlp(S, R), \]

where \( wp(S, true) \) characterises those states from which \( S \) is guaranteed to terminate. According to weakest precondition semantics a loop that may or may not terminate is indistinguishable from a loop that never terminates (both have a weakest precondition of \( false \) for any postcondition) but the two loops are distinguished by weakest liberal precondition semantics.

2.1. Basics

Let \( \text{Var} \) denote the universal set of variables that may take their values from a universal set of values, \( \text{Val} \), which includes the booleans, \( \mathbb{B} \). The set of all possible states, \( \Sigma \), is then defined as the set of all functions from \( \text{Var} \) to \( \text{Val} \). We assume that for every unprimed variable \( x \in \text{Var} \) there is also a primed copy \( x' \in \text{Var} \). The set of predicates \( \text{Pred} \) is defined as the set of all functions from states to booleans. We define the set of single-state predicates, \( \text{SPred} \), as the set of predicates that do not have any free primed variable. With the pointwise extension of the ordering \( \Rightarrow \) and the operators \( \lnot, \land, \lor \) from \( \mathbb{B} \), \( \text{Pred} \) and \( \text{SPred} \) become complete lattices. For two predicates \( P_1 \) and \( P_2 \) the entailment ordering \( \Rightarrow \) on \( \text{Pred} \) is implication for every state and \( \equiv \) is equivalence for every state. A predicate transformer is defined as a function from predicates to predicates that is monotonic with respect to the entailment ordering. Further details on the predicate space are given in Appendix A. The following definitions summarise the above.

\[
\begin{align*}
\Sigma &\overset{\text{def}}{=} \text{Var} \rightarrow \text{Val}, \\
\text{Pred} &\overset{\text{def}}{=} \Sigma \rightarrow \mathbb{B}, \\
P_1 \Rightarrow P_2 &\overset{\text{def}}{=} \forall \sigma(\sigma \in \Sigma \Rightarrow (P_1(\sigma) \Rightarrow P_2(\sigma))), \\
P_1 \equiv P_2 &\overset{\text{def}}{=} (P_1 \Rightarrow P_2) \land (P_2 \Rightarrow P_1).
\end{align*}
\]

2.2. The command language

Before defining our real-time programming language, we first define a set of primitive constructs in terms of which the rest of the language can be defined. Then we add contexts which allow variable declarations and typing information to be represented. Finally, we define our real-time language in terms of these primitives by adding a current time variable, \( \tau \).

Our primitive program constructs consist of the specification statement [29], here denoted \( x^{nt}[\mathcal{Q}] \), where the “\( nt \)” superscript denotes “nontimed” to distinguish it from the timed version below; an assumption about the program state denoted \( \{P\} \); nondeterministic choice over some set of commands indexed by set \( \mathcal{A} \), \( (\bigcap_{i \in \mathcal{A}} S_i) \); and sequential composition of commands, \( (S_1; S_2) \). Table 1 states the syntax and weakest liberal precondition semantics for the primitive commands. In the postcondition predicate \( R \), we do not allow references to primed variable names, i.e., \( R \in \text{SPred} \). The specification statement updates the variables in
its frame $x$ according to the predicate $Q \in \text{Pred}$. Note that the frame $x$ stands for a (possibly empty) set of variables that may be changed by this statement. The primed set of variables $x'$ denotes their final values. The predicate $Q$ may have free unprimed variables and only the free primed variables $x'$ corresponding to those that occur in the frame of the specification statement. In the semantics, variables $x$ are renamed $x'$ in predicate $R$ to match the final state naming convention used in predicate $Q$. The specification statement can describe the behaviour of assignment and other primitive programming statements [29]. For a predicate $P \in \text{SPred}$, statement $\{P\}$ allows an assumption about the program state to be included.

Nondeterministic choice over commands can be used to model conditional and iterative behaviour [2].

We extend the commands with a “context” predicate which is used to record invariants concerning the surrounding program. Such invariants are typically type declarations for variables of the form $v \in T$. A command $S$ is always seen in a certain (possibly true) context $C \in \text{SPred}$, expressed as $S^C$. Table 2 defines commands with contexts in terms of the primitive commands. For a specification statement the context is assumed to hold in the initial state and in the final state. Contexts in this sense are similar to the invariants introduced by Morgan and Vickers [31]. An assumption occurring in a particular context always assumes that the context predicate holds. Contexts are carried through nondeterministic choice, nesting and sequential composition in obvious ways.

As well as the commands in Table 2, a variable declaration $(\text{var } v : T \cdot S_1)^C$ extends statement $S_1$’s context $C$ by introducing the fact that new variable $v$ has type $T$, and that the original context $C$ holds in the presence of this newly-declared variable. The type $T$ of a variable must be a nonempty subset of $\text{Val}$. The weakest liberal precondition of a variable
Table 3
Real-time commands

<table>
<thead>
<tr>
<th>Command $S$</th>
<th>Equivalent command</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x;[Q]$</td>
<td>$x, \tau^{nf} [Q \land \tau \leq \tau']$</td>
</tr>
<tr>
<td>$[Q]$</td>
<td>$\emptyset;[Q]$</td>
</tr>
</tbody>
</table>

block is defined as follows:

$$wlp((\text{var } v : T \bullet S_1)^C, R) \equiv (\forall v(wlp(S_1^{v \in T \wedge C[w/v]}, R[w/v]))[v/w]$$

where $w \in \text{Indep}(R)$ and $w \notin \text{Idf}((\text{var } v : T \bullet S_1)^C)$.

A substitution with a fresh variable $w$ is performed in context $C$ and predicate $R$ to exclude unwanted bindings to an externally declared variable with name $v$, if any. In the proviso, $\text{Indep}(R)$ is the set of variable identifiers that the predicate $R$ does not depend on (see Appendix A for more details) and $\text{Idf}(S)$ denotes those variable identifiers that appear free in command $S$ (see Table A.1 for a full definition).

Table 3 extends the language further with the abstract syntax and semantics of a timed specification statement, $x;[Q]$. A timed specification statement is defined with the help of a conventional specification statement and an additional variable $\tau$ that refers to the current time and ranges over the real numbers $\mathbb{R}$. The timed specification statement implicitly has the reserved current time variable $\tau$ in its frame, plus the additional condition $\tau \leq \tau'$, making sure that the time never goes backwards. The frame $x$ of the timed specification statement denotes a possibly empty set of variables that are distinct from $\tau$. The timed specification statement is the primitive construct for ‘timed’ commands [20].

Definition 2.1 (Timed command). A timed command denotes a command $S^C$, with a context $C$ such that $C \Rightarrow \tau \in \mathbb{R}$, that is constructed from variable declarations and the program constructors in the first column of Table 2 with timed specification statements instead of nontimed ones.

Finally, coercions $[Q]$ are defined as timed specification statements with an empty frame.

Other commands may be modelled using timed commands. For example, the idle command, that changes no variables but may consume time, and a (timed) conditional command may be modelled as follows:

idle $\equiv [true],$

if $B$ then $S_1$ else $S_2$ fi $\equiv ([B]; S_1; \text{idle}) \sqcap ([\neg B]; S_2; \text{idle}),$ \hspace{1cm} (1)

where we have used the infix operator “$\sqcap$” as a shorthand for a choice over two alternatives. Notice how this decomposes the conditional into its two possible paths. In dealing with the timing analysis of such commands it is desirable to treat each path separately because they may have quite different timing characteristics. Note that an individual path, such as $([B]; S_1; \text{idle})$, is miraculous (or infeasible) in initial states in which $B$ does not hold and hence that path is not followed. Further commands are defined in Tables 6 and 7.
3. Command entry and traversal conditions

The execution time of a command, $S$, may depend on the initial state (of the program’s variables). However, we need to consider two exceptional cases: in some states, (a) the command executes forever or (b) the command is miraculous [9]. In both cases, we are not interested in the execution time because (a) the command does not terminate or (b) the command corresponds to a path that is not followed. In the weakest liberal precondition semantics these alternatives are not distinguished. They both correspond to the states satisfying $wlp(S, false)$. Recall that $wlp(S, R)$ defines those initial states from which, if $S$ terminates, it does so in a state that satisfies $R$. Hence, $wlp(S, false)$ corresponds to those initial states from which $S$ does not terminate, or if it does, the state satisfies false, i.e., it is miraculous from that initial state. For execution-time analysis we are interested in the initial states that may lead to nonmiraculous termination, which we refer to as the entry condition, $E(S)$, of command $S$.

**Definition 3.1 (Entry condition).** The entry condition, $E(S)$, of a command, $S$, is defined as the predicate $¬wlp(S, false)$.

If there are no states that satisfy a command’s entry condition it is a dead command [18].

**Definition 3.2 (Dead command).** A command $S$ is dead iff $E(S) ≡ false$.

For a sequential composition, $(S_1; S_2)$, the calculation of its entry condition $E(S_1; S_2)$ gives the following:

$¬wlp((S_1; S_2), false) ≡ ¬wlp(S_1, wlp(S_2, false)) ≡ ¬wlp(S_1, ¬E(S_2)).$  

(2)

This motivates a generalisation of the entry condition that defines the traversal condition for a command $S$ as a restriction of the entry condition to those states from which $S$ can possibly achieve a state satisfying postcondition $R$.

**Definition 3.3 (Traversal condition).** The traversal condition $E(S, R)$ of a command $S$, for $R ∈ SPred$, is defined as the predicate $¬wlp(S, ¬R)$.

Note that $E(S) ≡ E(S, true)$, i.e., the entry condition is the traversal condition to terminate in any state. The entry condition for the sequential composition (2) can now be written as $E(S_1, E(S_2, true))$. Note that $E(S, R)$ is monotonic with respect to entailment on $R$, i.e., if $R ⇒ R’$ then $E(S, R) ⇒ E(S, R’)$.

**Theorem 3.4 (Traversal condition).** Table 4 defines the traversal condition $E(S, R)$ for commands $S$ and predicates $R ∈ SPred$.

The proof is by expanding the definition of the traversal condition.

For example, let $B ∈ SPred$ with $τ ∈ Independ(B)$. By assuming that the entry condition for $S_1^C$ is $C$, the entry condition for the first alternative of the conditional (1) in context...
Table 4
Computation of the traversal condition $\mathcal{E}(S, R)$

<table>
<thead>
<tr>
<th>Command $S$</th>
<th>$\mathcal{E}(S, R)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x{:}\text{nt}[Q])^C$</td>
<td>$\exists x' (C \land (C \land R)[x'/x] \land Q)$</td>
</tr>
<tr>
<td>$[P]^C$</td>
<td>$P \land C \land R$</td>
</tr>
<tr>
<td>$(\text{var } v : T \bullet S_1)^C$</td>
<td>$(\exists v \mathcal{E}(S_1^v \in T \land C[w/v]), R[w/v])[w/v]$ with $w \not\in \text{Idf}(S)$ and $w \in \text{Indep}(R)$</td>
</tr>
<tr>
<td>$(\bigwedge_{i\in A} S_i)^C$</td>
<td>$\bigvee_{i\in A} \mathcal{E}(S_i^C, R)$</td>
</tr>
<tr>
<td>$(S_1; S_2)^C$</td>
<td>$\mathcal{E}(S_1^C, \mathcal{E}(S_2^C, R))$</td>
</tr>
</tbody>
</table>

$C \equiv \tau \in \mathbb{R}$ can be calculated as follows:

$$
\mathcal{E}([B]; S_1; \text{idle})^C, \text{true}) \equiv \mathcal{E}([B]^C, \mathcal{E}(S_1^C, \mathcal{E}(\text{idle}^C, \text{true}))) \\
\equiv \mathcal{E}([B]^C, \mathcal{E}(S_1^C, C)) \\
\equiv \mathcal{E}([B]^C, C) \\
\equiv B \land C.
$$

Similarly, assuming $\mathcal{E}(S_2^C) \equiv C$, the entry condition for the second alternative is $\neg B \land C$, and the entry condition for the whole conditional is $(B \land C) \lor (\neg B \land C) (\equiv C)$.

4. Liberal command refinement

We define a liberal program refinement relation on the command language via the weakest liberal precondition semantics by interpreting a command as a predicate transformer on the subspace consisting of all predicates in $\text{SPred}$. This refinement relation ensures partial correctness in program development. All functions on predicates that have been used to define the semantics of commands in Table 2 are monotone functions and the restrictions on the program statements ensure that the underlying predicate transformers map predicates from $\text{SPred}$ to predicates in $\text{SPred}$.

**Definition 4.1 (Liberal refinement).** Let $S_1, S_2$ be two commands. We say that $S_2$ **liberally refines** $S_1$ and write $S_1 \sqsubseteq_{\text{wlp}} S_2$ if $\text{wlp}(S_1, R) \Rightarrow \text{wlp}(S_2, R)$ for all predicates $R \in \text{SPred}$. Liberal refinement equivalence of $S_1$ and $S_2$ is denoted by $S_1 \sqsubseteq_{\text{wlp}} S_2$.

Note that liberal refinement is different from common refinement relations based on weakest preconditions used in total correctness approaches [1,30]. A refinement $S \sqsubseteq_{\text{wlp}} S'$ means that the predicate characterising the entry condition of command $S'$, is stronger than the one for command $S$, and furthermore, that all states that command $S'$ can achieve are possible ones for command $S$. Every liberal refinement decreases nondeterminism and strengthens the entry condition. Unlike refinement based on weakest preconditions (total correctness), liberal refinement may increase the domain of nontermination.
5. Symbolic computation of execution times

This section focuses on timed commands. We show how worst-case and best-case execution times for timed commands can be defined and computed on the basis of the underlying weakest liberal precondition semantics.

5.1. Infimum and supremum

Our theory relies on the notions of infimum and supremum. As with predicates (which are defined to be functions from states to booleans) our definitions of supremum and infimum are also functions from the state. We use the notation \( \sup \{ \mathcal{V} | B \bullet \theta \} \) to denote the supremum (least upper bound) of function \( \theta \in \Sigma \rightarrow (\mathbb{R} \cup \{\infty, -\infty\}) \) over all states \( \sigma' \), where predicate \( B \) holds that may differ from state \( \sigma \) only in the variables \( \mathcal{V} \). The infimum is defined similarly. Note that \( \sup \{ \mathcal{V} | B \bullet \theta \} \) is of type \( \Sigma \rightarrow (\mathbb{R} \cup \{\infty, -\infty\}) \). The domain \( \mathbb{R} \) must be extended with infinite values \( \infty \) and \( -\infty \) here to account for situations where no finite bound exists. In particular, the supremum (infimum) of the empty set is defined to be \( -\infty \) (\( \infty \)). We also use the notation \( \sup_{\theta \in \Omega} \theta(\sigma) \) to denote the supremum of the set of expressions \( \theta(\sigma) \), for \( \theta \) ranging over a set of functions \( \Omega \), and a similar notation for the infimum. Appendix A contains the formal definition of these notations.

5.2. Defining time bounds

As a motivational example the assignment of value 1 to variable \( x \) taking between one and two time units can be specified as the timed specification statement

\[
x: [x' = 1 \land 1 \leq \tau' - \tau \leq 2].
\]  

(3)

This command has “worst-case” execution time 2 and “best-case” execution time 1. To formally derive the execution time of a timed command, \( S \), we introduce a fresh variable, \( \xi \), to stand for the termination time of the command. Then \( \mathcal{E}(S, \xi = \tau) \) is a predicate (in \( \xi \) and the initial state variables) representing those initial states from which \( S \) can possibly terminate at time \( \xi \). The current time in the initial state is \( \tau \), and hence \( \xi - \tau \) represents the execution time of \( S \). To determine the worst-case (best-case) execution time, we take the supremum (infimum) over \( \xi \) of \( \xi - \tau \) for states satisfying the \( \mathcal{E}(S, \xi = \tau) \). Let \( \mathcal{W}(S) \) and \( \mathcal{B}(S) \) be the worst- and best-case execution times of command \( S \), respectively,

\[
\mathcal{W}(S) \overset{\text{def}}{=} \sup \{ \xi | \mathcal{E}(S, \xi = \tau) \bullet \xi - \tau \},
\]

\[
\mathcal{B}(S) \overset{\text{def}}{=} \inf \{ \xi | \mathcal{E}(S, \xi = \tau) \bullet \xi - \tau \}.
\]  

(4)

For the example (3) above we get its worst-case execution time, \( \mathcal{W}(S) \), as

\[
\sup \{ \xi | \mathcal{E}(x: [x' = 1 \land 1 \leq \tau' - \tau \leq 2], \xi = \tau) \bullet \xi - \tau \}
\]

\[
= \sup \{ \xi | \exists x', \tau'(x' = 1 \land 1 \leq \tau' - \tau \leq 2 \land \xi = \tau') \bullet \xi - \tau \}
\]

\[
= \sup \{ \xi | 1 \leq \xi - \tau \leq 2 \bullet \xi - \tau \}
\]

\[
= 2.
\]

Similarly, its best-case execution time can be calculated as 1. \( \mathcal{W}(S) \) and \( \mathcal{B}(S) \) are expressions on the initial state (including \( \tau \)). To calculate the worst-case execution time over all initial
states one needs to take the supremum of $\mathcal{W}(S)(\sigma)$ over all states $\sigma$. For the example (3) above $\mathcal{W}(S)$ is independent of the state and hence $\mathcal{W}(S)(\sigma)$ is 2 for all states.

If $S$ is dead then $E(S, true) \equiv false$, and because the traversal condition is monotone on $SPred$, $E(S, \xi = \tau) \Rightarrow E(S, true)$ and hence $E(S, \xi = \tau) \equiv false$. Therefore, the worst-case execution time for a dead command is given by

$$\sup\{\xi | E(S, \xi = \tau) \bullet \xi - \tau\} = \sup\{\xi | false \bullet \xi - \tau\} = -\infty.$$  

The determination of the worst-case execution time of a sequential composition, $(S_1; S_2)$, is, unfortunately, not as simple as summing the respective worst-case execution times of the two statements. There are two reasons for this. Firstly, $S_1$ may terminate in a state that does not satisfy the entry condition for $S_2$. Hence, when determining the worst-case execution time for $S_1$, we need to restrict our attention to initial states from which $S_1$ can achieve states satisfying the entry condition for $S_2$, that is, initial states satisfying $E(S_1, E(S_2))$. Secondly, the worst-case execution time of $S_2$ depends on its initial state. The predicate

$$E(S_1, E(S_2) \land \xi = \tau + \mathcal{W}(S_2))$$

characterises those initial states from which $S_1$ can reach a state $\sigma$ which (a) satisfies the entry condition for $S_2$, and (b) in which $\xi$ is equal to the worst-case execution time of $S_2$ from state $\sigma$ plus the termination time of $S_1$, i.e., $\tau$. Hence,

$$\mathcal{W}(S_1; S_2) = \sup\{\xi | E(S_1, E(S_2) \land \xi = \tau + \mathcal{W}(S_2)) \bullet \xi - \tau\}.$$  

(5)

Theorem 5.2 proves that this corresponds with our definition (4) of worst-case execution time.

5.3. Calculating time bounds

To allow systematic (symbolic) calculation of the worst-case execution time of a sequence (or path) of commands, we generalise function $\mathcal{W}(S_1)$ to function $\mathcal{W}(S_1, R, \theta)$, which represents the worst-case execution time of the path consisting of $S_1$ followed by some path $S_2$, where $R$ is a predicate representing the entry condition for path $S_2$ and $\theta$ represents the worst-case execution time of path $S_2$. Note that $\theta$ is a function of the state. With this definition, the worst-case execution time in Eq. (5) can be written as $\mathcal{W}(S_1, E(S_2), \mathcal{W}(S_2))$.

**Definition 5.1 (Execution-time bounds).** Let $S$ be a timed command, let $\theta \in \Sigma \rightarrow (\mathbb{R} \cup \{\infty, -\infty\})$ and let $R \in SPred$ and let $\xi \in Var$ with $\xi \notin Idf(S)$ and $\xi \in Independ(R) \cap Independ(0)$. The best-case and worst-case execution time expressions $B(S, R, \theta)$ and $\mathcal{W}(S, R, \theta)$ are of type $\Sigma \rightarrow (\mathbb{R} \cup \{\infty, -\infty\})$ and are defined by

$$B(S, R, \theta) \overset{\text{def}}{=} \inf\{\xi | E(S, R \land \xi = \tau + \theta) \bullet \xi - \tau\}$$

and

$$\mathcal{W}(S, R, \theta) \overset{\text{def}}{=} \sup\{\xi | E(S, R \land \xi = \tau + \theta) \bullet \xi - \tau\}.$$
Table 5
Computation of the worst-case execution time $\mathcal{W}(S, R, \theta)$

<table>
<thead>
<tr>
<th>Command $S$</th>
<th>$\mathcal{W}(S, R, \theta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x: [Q])^C$</td>
<td>$\sup_\tau \xi: \mathcal{E}((x: [Q])^C, R \wedge \xi = \tau + \theta) \cdot \xi - \tau$</td>
</tr>
<tr>
<td>${P}^C$</td>
<td>$\sup_\xi \left{ \exists \tau', x': (C \wedge (C \wedge R)[x', \tau'/x, \tau] \wedge Q \wedge \tau' \leq \tau' \cdot \theta[x', \tau'/x, \tau] + \tau' - \tau) \wedge \xi = \tau + \theta \cdot \xi - \tau \right}$</td>
</tr>
<tr>
<td>$(\text{var } v : T \bullet S_1)^C$</td>
<td>$\sup_\xi \left{ \exists \tau', x': (C \wedge (C \wedge R)[x', \tau'/x, \tau] \wedge Q \wedge \tau' \leq \tau' \cdot \theta[x', \tau'/x, \tau] + \tau' - \tau) \wedge \xi = \tau + \theta \cdot \xi - \tau \right}$</td>
</tr>
<tr>
<td>$(\bigcap_{i \in A} S_i)^C$</td>
<td>$\sup_{i \in A} \mathcal{W}(S_i^C, R, \theta)$</td>
</tr>
<tr>
<td>$(S_1^C \cup C_2)$</td>
<td>$\mathcal{W}(S_1^C \cup C_2, R, \theta)$</td>
</tr>
<tr>
<td>$(S_1; S_2)^C$</td>
<td>$\mathcal{W}(S_1^C \cup C_2, R, \theta)$</td>
</tr>
</tbody>
</table>

Note that $\mathcal{W}(S) = \mathcal{W}(S, true, 0)$ and $\mathcal{B}(S) = \mathcal{B}(S, true, 0)$, where “0” here represents the function that is zero in all states.

Table 5 provides a method for the symbolic computation of worst-case execution times of timed commands.

**Theorem 5.2 (Execution-time bounds).** Let $S$ be a timed command, $R \in \text{SPred}$ and $\theta \in \Sigma \rightarrow (\mathbb{R} \cup \{-\infty, +\infty\})$, then Table 5 defines $\mathcal{W}(S, R, \theta)$.

**Proof.** We prove the assertion of the theorem by induction on the structure of a timed command $S^C$ with context $C$. The proof for specification statements $x: [Q]$ is as follows:

$$\mathcal{W}(x: [Q])^C, R, \theta$$

= $\sup_\xi \left\{ \mathcal{E}(x: [Q])^C, R \wedge \xi = \tau + \theta \right\} \cdot \xi - \tau$

“By Table 4”

= $\sup_\xi \left\{ \exists \tau', x': (C \wedge (C \wedge R)[x', \tau'/x, \tau] \wedge Q \wedge \tau' \leq \tau' \cdot \theta[x', \tau'/x, \tau] + \tau' - \tau) \wedge \xi = \tau + \theta \cdot \xi - \tau \right\}$

“By Theorem C.1”

= $\sup_\tau \sup_\xi \left\{ \mathcal{E}(S_1^C \cup C, R, \theta) \right\} \cdot \xi - \tau$

The proof for assumptions $\{P\}$ is trivial. Next, we show the induction step for variable declarations. We fix a variable $w$ with $w \notin \text{Idf}(S)$ and $w \in \text{Indep}(R) \cap \text{Indep}(\theta)$.

$$\mathcal{W}(\text{var } v : T \bullet S_1)^C, R, \theta$$

= $\sup_\xi \left\{ \exists \tau', x': (C \wedge (C \wedge R)[x', \tau'/x, \tau] \wedge Q \wedge \tau' \leq \tau' \cdot \theta[x', \tau'/x, \tau] + \tau' - \tau) \wedge \xi = \tau + \theta \cdot \xi - \tau \right\}$

“By Table 4”

= $\sup_\xi \left\{ \exists \tau', x': (C \wedge (C \wedge R)[x', \tau'/x, \tau] \wedge Q \wedge \tau' \leq \tau' \cdot \theta[x', \tau'/x, \tau] + \tau' - \tau) \wedge \xi = \tau + \theta \cdot \xi - \tau \right\}$

“By Theorem C.1”

= $\sup_\xi \left\{ \mathcal{E}(S_1^C \cup C, R, \theta) \right\} \cdot \xi - \tau$

“By induction hypothesis”

$\sup_\xi \left\{ \mathcal{W}(S_1^C \cup C, R, \theta) \right\} \cdot \xi - \tau$. 

+∞
The induction step for nondeterministic choice \((\bigcap_{i \in A} S_i)\) is as follows:

\[
\begin{align*}

\mathcal{W}\left(\left(\bigcap_{i \in A} S_i\right)^C, R, \theta\right) &= \sup \left\{ \xi \mid \sup_{i \in A} \left(\left(\bigcap_{i \in A} S_i\right)^C, R \wedge \xi = \tau + \theta\right) \cdot \xi - \tau \right\} \\
&= \sup \left\{ \xi \mid \sqrt{\sup_{i \in A} \mathcal{E}(S_i^C, R \wedge \xi = \tau + \theta) \cdot \xi - \tau \right\} \\
&= \sup_{i \in A} \left\{ \xi \mid \sup_{\eta} \mathcal{E}(S_i^C, R \wedge \eta = \tau + \theta) \cdot \eta - \xi \right\} \\
&= \sup_{i \in A} \left\{ \xi \mid \sup_{\eta} \mathcal{E}(S_i^C, R \wedge \eta = \tau + \theta) \cdot \eta - \xi \right\} \\
&= \sup_{i \in A} \left\{ \xi \mid \sup_{\eta} \mathcal{E}(S_i^C, R \wedge \eta = \tau + \theta) \cdot \eta - \xi \right\}
\end{align*}
\]

It remains to show the induction step for sequential composition, \((S_1; S_2)\). According to Theorem B.5, we can assume that there is a timed specification statement \(x : \{Q\}\) which is liberal refinement equivalent to \(S_1^C\).

\[
\begin{align*}

\mathcal{W}(S_1^C, E(S_2^C), R), \mathcal{W}(S_2^C, R, \theta))
&= \text{“By Definition 5.1 of } \mathcal{W} \text{ on } S_1^C” \\
&= \sup(\xi \mid E(S_1^C, E(S_2^C), R \wedge \xi = \tau + \mathcal{W}(S_2^C, R, \theta)) \cdot \xi - \tau)
\end{align*}
\]

\[
\begin{align*}

&= \text{“By Definition 5.1 of } \mathcal{W} \text{ on } S_2^C” \\
&= \sup(\xi \mid E(S_1^C, E(S_2^C), R)) \\
&= \text{“By Table 4 assuming } S_1^C \text{ is equivalent to } x : \{Q\}\text{”} \\
&= \text{“By Theorem C.1; also cancelling out } \tau” \\
&= \sup(\xi, \tau', x' \mid Q \wedge \tau \leq \tau' \wedge E(S_2^C, R)[\tau', x'/\tau, x]) \\
&= \text{“By monotonicity of the command traversal condition”} \\
&= \sup(\xi, \tau', x' \mid Q \wedge \tau \leq \tau' \wedge E(S_2^C, R)[\tau', x'/\tau, x]) \\
&= \text{“By Theorem C.1”} \\
&= \sup(\xi, \tau', x' \mid Q \wedge \tau \leq \tau' \wedge E(S_2^C, R)[\tau', x'/\tau, x]) \\
&= \text{“By Table 4 assuming } S_1^C \text{ is equivalent to } x : \{Q\}\text{”} \\
&= \sup(\xi \mid E(S_1^C, E(S_2^C), R \wedge \xi = \tau + \theta)) \cdot \xi - \tau)
\end{align*}
\]
By Table 4
\[ \sup\{\xi \mid \mathcal{E}(S_1; S_2)^C, R \land \xi = \tau + \theta \} \bullet \xi - \tau \]
= “By Definition 5.1”
\[ \mathcal{W}(S_1; S_2)^C, R, \theta). \]

A similar theorem holds for the best-case execution time: by replacing the expression \( \mathcal{W}(S, R, \theta) \) with \( \mathcal{B}(S, R, \theta) \) and the supremum with the infimum in all expressions in Table 5 we obtain a method for the symbolic computation of best-case execution times.

A consequence of the definition of timed commands, worst-case and best-case execution times and the previous theorem are the following correspondences.

**Theorem 5.3 (Achievable execution times).** For every timed command \( S \) and predicate \( R \in \text{SPred} \), it is the case that

- \( \mathcal{B}(S, R, 0) \geq 0 \),
- \( \mathcal{E}(S, R) \equiv (\mathcal{B}(S, R, 0) \leq \mathcal{W}(S, R, 0)) \),
- \( \neg \mathcal{E}(S, R) \equiv \mathcal{B}(S, R, 0) = \infty \), and
- \( \neg \mathcal{E}(S, R) \equiv \mathcal{W}(S, R, 0) = -\infty \).

In other words, no command takes a negative time, the best-case execution time never exceeds the worst-case one on states that fulfil the traversal condition, and the execution times are unsatisfiable on states that do not fulfil the traversal condition.

**5.4. Refining time bounds**

Any liberal refinement \( S \sqsubseteq_{\text{wlp}} S' \) always tightens the worst-case and the best-case execution times of a timed command \( S \) in the sense that the worst-case execution time of \( S' \) is below the one for \( S \) and the best-case execution time of \( S' \) is above the one for \( S \). This is stated in the following theorem which is derived from Definition 5.1 and the fact that \( \mathcal{E}(S', R) \Rightarrow \mathcal{E}(S, R) \) for any predicate \( R \in \text{SPred} \).

**Theorem 5.4 (Time-bound refinement).** Let \( S, S' \) be timed commands with \( S \sqsubseteq_{\text{wlp}} S' \), let \( R \in \text{SPred} \) and let \( \theta \) be a function on \( \Sigma \) with values in \( \mathbb{R} \cup \{-\infty, \infty\} \). Then, \( \mathcal{B}(S, R, \theta) \leq \mathcal{B}(S', R, \theta) \) and \( \mathcal{W}(S', R, \theta) \leq \mathcal{W}(S, R, \theta) \).

This shows that program development with liberal refinement (partial correctness) preserves upper bounds for worst-case and lower bounds for best-case execution-time behaviour. This is not necessarily the case for refinement based on weakest preconditions (total correctness), since states from where the program may not terminate can then become states from where anything can happen.

**6. Example**

This section applies our techniques to the timing analysis of a “message transmitter” example. Timing constraints are extracted from the high-level program, and the compiled
Table 6
High-level language commands and equivalent modelling language commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Wlp-command equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x := E$</td>
<td>$x: [x' = E]$</td>
</tr>
<tr>
<td>deadline $D$</td>
<td>$[\tau' = \tau \land \tau \leq D]$</td>
</tr>
<tr>
<td>delay until $D$</td>
<td>$[D \leq \tau' \leq \max(\tau, D) + \text{late}]$</td>
</tr>
<tr>
<td>while $G$ do $S$ end</td>
<td>$(\forall i \in \mathbb{N}; S_i; \neg G)$</td>
</tr>
<tr>
<td></td>
<td>where $S_0 \overset{\text{def}}{=} [\tau' = \tau]$ and $S_{i+1} \overset{\text{def}}{=} [G]; S_i$, for $i \in \mathbb{N}$</td>
</tr>
</tbody>
</table>

Fig. 2. High-level language transmitter program.

```
var msg : array(0..size - 1) of nat;
  out : nat;
  n : nat;
;
{\tau \leq 30};
n := 0;
while n \neq size do
  out := msg(n);
  deadline 50 + 35 \times n;
  delay until 56 + 35 \times n;
  n := n + 1
end;
deadline 56 + 35 \times size
```

6.1. The message transmitter

To illustrate the execution time computation techniques on a high-level real-time program, Fig. 2 contains a simplified version of a program which displays a message of size characters,
one character at a time, in a shared memory location, \textit{out}, under the constraint that the first character must be displayed from (at least) time 50 to time 56, the second character must be displayed from time 85 to time 91, and so on \cite{19}. A new character appears every 35 \(\mu\)s, and remains visible for at least 6 \(\mu\)s. The \textit{delay until} statement forces the character to remain visible for the required time, and the \textit{deadline} states that the program must have produced the character by the required time.

The challenge when verifying such a program is to show that the timing of each control-flow path ending at a deadline command ensures that the deadline will always be met. As an example of a timing path in this program, we investigate the control-flow path that starts with the assumption at the beginning of the program, enters the while loop for the first time and ends with the first deadline command. We denote this path by \textit{Path A}.

\[ \{ \tau \leq 30 \}; \]
\[ n := 0; \]
\[ [n \neq \text{size}]; \]
\[ \text{out} := \text{msg}(n); \]
\[ \text{deadline} 50 + 35 \times n \]

Note that in \textit{Path A}, the coercion statement \([n \neq \text{size}]\) records the condition that has to be true for the loop to be entered \cite{18}.

This is, of course, only one of the many paths through such a program. In particular, to successfully prove the timing correctness of an embedded program it is usually necessary to prove that each process iterates quickly enough to process data at the correct rate. For instance, in this case we would also want to analyse the path that goes from the deadline of \(50 + 35 \times n\), around the “loop”, and back to itself, in order to prove that the task can achieve its required periodicity. We do not go further into the issue of finding all relevant timed paths and the problem of extracting a minimal set of primitive paths that have to be analysed to derive a sufficient set of timing constraints \cite{15,17}.

The following predicate defines the program context \(C\) for \textit{Path A}.

\[ C \overset{\text{def}}{=} \tau \in \mathbb{R} \land \text{out}, n \in \mathbb{N} \land \text{msg} \in \{0, \ldots, \text{size} - 1\} \rightarrow \mathbb{N}. \]

In this context (which is implicit below), we compute the traversal condition of \textit{Path A} to achieve \(\zeta = \tau\) as follows, by calculating backwards up the path with the help of Table 4,

\[ \mathcal{E}(\text{deadline} 50 + 35 \times n, \zeta = \tau) \]
\[ \equiv \tau \leq 50 + 35 \times n \land \zeta = \tau \]
\[ \mathcal{E}(\text{out} := \text{msg}(n), \tau \leq 50 + 35 \times n \land \zeta = \tau) \]
\[ \equiv \exists \tau', \text{out}' (\tau \leq \tau' \land \text{out}' = \text{msg}(n) \land \tau' \leq 50 + 35 \times n \land \zeta = \tau') \]
\[ \equiv \tau \leq \zeta \leq 50 + 35 \times n \]
\[ \mathcal{E}([n \neq \text{size}], \tau \leq \zeta \leq 50 + 35 \times n) \]
\[ \equiv \exists \tau' (\tau \leq \tau' \land n \neq \text{size} \land \tau' \leq \zeta \leq 50 + 35 \times n) \]
\[ \equiv n \neq \text{size} \land \tau \leq \zeta \leq 50 + 35 \times n \]
\[ \mathcal{E}(n := 0, n \neq \text{size} \land \tau \leq \zeta \leq 50 + 35 \times n) \]
\[ \equiv \exists \tau', n' (\tau \leq \tau' \land n' = 0 \land n' \neq \text{size} \land \tau' \leq \zeta \leq 50 + 35 \times n') \]
\[ \equiv \tau \leq \zeta \leq 50 \land 0 \neq \text{size} \]
\[ E(\{\tau \leq 30\}, \tau \leq \xi \leq 50 \land 0 \neq \text{size}) \equiv \tau \leq 30 \land \tau \leq \xi \leq 50 \land 0 \neq \text{size} \equiv E(\text{Path A}, \xi = \tau). \]

This is exactly the condition we require to traverse this path with termination time \( \xi \). The starting time \( \tau \) is not later than 30 and the length of the message is not 0 (which is necessary to enter the loop at least once) and \( \xi \) must be not greater than 50. The worst-case execution time of \text{Path A} is computed with the help of Definition 5.1 as follows:

\[
\mathcal{W}(\text{Path A}) = \sup\{\xi \mid E(\text{Path A}, \xi = \tau) \cdot \xi - \tau\} = \sup\{\xi \mid \tau \leq 30 \land \tau \leq \xi \leq 50 \land 0 \neq \text{size} \cdot \xi - \tau\} = \begin{cases} 50 - \tau & \tau \leq 30 \land 0 \neq \text{size}, \\ -\infty & \text{otherwise.} \end{cases}
\]

To interpret this result, consider that the path is not permitted to start later than time 30. The computed expression \( 50 - \tau \) specifies the uppermost execution time of the path with respect to the starting time \( \tau \). In the worst case, when the program starts at time 30, the path can take no more than 20 \( \mu \)s. Importantly, if we can prove that an implementation of this path never takes more than 20 time units, the deadline at the end will always be met for any anticipated starting time. However, if the path starts too late or \text{size} equals 0, then there is no timing obligation on the path.

6.2. Analysing the transmitter implementation

Fig. 3 depicts an implementation of the transmitter program in MIPS-like assembler language. Here, \text{msg} and \text{out} are symbolic constants representing the addresses allocated to these high-level language variables. Expression \( i \) denotes register number \( i \) and function \text{clock} denotes the machine clock. The \text{clock} is modelled as an input to the program which keeps track of the actual time. However, since the instruction that samples the clock takes 1 \( \mu \)s the sampled time \text{clock} is slightly behind the actual time \( \tau \). The assembler commands are defined in Table 7 on the base of our modelling language. We assume an abstract machine with a register function \( r \) on the set of registers \( \text{Reg} \defeq \{0, \ldots, 31\} \) and a memory function \( m \) on the set of addresses (natural numbers) \( \text{Addr} \), both with values in the set of machine representations (integers) \( \text{Int} \). Every assembler command \( S \) has a machine address \( l \) in \( \text{Addr} \) denoted by \( l : S \). The program counter (pc) ranges over these addresses. In addition, execution times have been given to each of the commands. For simplicity, we have not included any caching or pipelining effects. The following defines the context of the assembler program in Fig. 3:

\[
C \defeq \tau \in \mathbb{R} \land \text{msg}, \text{out}, \text{pc} \in \text{Addr} \land m \in \text{Addr} \rightarrow \text{Int} \land r \in \text{Reg} \rightarrow \text{Int} \\
\land \text{clock} \in \mathbb{R} \rightarrow \text{Int} \land \text{Addr} \subseteq \text{Int} \land \tau - 1 \leq \text{clock}(\tau) \leq \tau.
\]

On the base of the timing behaviour of the assembler program we can now compare the high-level timing constraints of the transmitter with the actual execution times of its
Table 7
Assembler commands and defining modelling language commands

<table>
<thead>
<tr>
<th>Assembler commands</th>
<th>Equivalent modelling language command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lb Si, a</code></td>
<td><code>r, pc:[r' = r ⊕ [i → m(a)] ∧ τ' = τ + 1 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>lb Si, (Sj)</code></td>
<td><code>r, pc:[r' = r ⊕ [i → m(r(j))] ∧ 1 ≤ τ' − τ ≤ 3 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>li Si, z</code></td>
<td><code>r, pc:[r' = r ⊕ [i → z] ∧ τ' = τ + 1 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>lt Si, clock</code></td>
<td><code>r, pc:[r' = r ⊕ [i → clock(τ)] ∧ τ' = τ + 1 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>sb Si, a</code></td>
<td><code>pc, m:[m' = m ⊕ [a → r(i)] ∧ τ' = τ + 2 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>ja</code></td>
<td><code>pc:[τ' = τ + 1 ∧ pc' = a]</code></td>
</tr>
<tr>
<td><code>bgtz Si, a</code></td>
<td><code>pc: [(r(i) ≤ 0 ⇒ pc' = pc + 1) ∧ (r(i) &gt; 0 ⇒ pc' = a) ∧ 1 ≤ τ' − τ ≤ 2]</code></td>
</tr>
<tr>
<td><code>bne Si, Sj, a</code></td>
<td><code>pc: [(r(i) ≠ r(j) ⇒ pc' = a) ∧ (r(i) = r(j) ⇒ pc' = pc + 1) ∧ 1 ≤ τ' − τ ≤ 2]</code></td>
</tr>
<tr>
<td><code>add Si, Sj, Sk</code></td>
<td><code>r, pc: [r' = r ⊕ [i → r(j) − r(k)] ∧ τ' = τ + 1 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>addi Si, Sj, z</code></td>
<td><code>r, pc: [r' = r ⊕ [i → r(j) + z] ∧ τ' = τ + 1 ∧ pc' = pc + 1]</code></td>
</tr>
<tr>
<td><code>l: S</code></td>
<td><code>[pc = l ∧ τ = τ']</code></td>
</tr>
</tbody>
</table>

Address `a`, registers `Si, Sj, Sk`, integer `z` and program counter address `l`.

```
--{τ ≤ 30}
20: li $0, msg $0 := msg base address
21: li $1, size $1 := size (length of msg)
22: li $2, 0 $2 := 0 (loop counter n)
23: li $3, 56 $3 := 56 (first delay time)
24: li $4, 35 $4 := 35 (separation time)
25: j 34 goto loop test
26: add $5, $2, $0 $5 := n + msg base
27: lb $6, ($5) $6 := msg(n)
28: sb $6, out out := msg(n)
29: lt $7, clock $7 := current time
30: sub $7, $3, $7 $7 := delay time − current time
31: bgtz $7, 29 delay if $7 > 0
32: add $3, $3, $4 delay time := delay time + 35
33: addi $2, $2, 1 increment n
34: bne $1, $2, 26 goto loop body if n ≠ size
```
Fig. 3. MIPS-like assembler code of the message transmitter.
implementation. The following control-flow path through the assembler code corresponds to Path A of the high-level program. We call this program path Path B.

\[ \tau \leq 30 \]

20: \texttt{li} $0, \text{msg}$
21: \texttt{li} $1, \text{size}$
22: \texttt{li} $2, 0$
23: \texttt{li} $3, 56$
24: \texttt{li} $4, 35$
25: \texttt{j} 34
26: \texttt{bne} $1, 2, 26$
27: \texttt{add} $5, 2, 1$
28: \texttt{sb} $6, \text{out}$

The computation of the traversal condition of Path B is outlined below. Any command with machine address \( i \) is referenced under the name \( S_i \). The equivalences hold under context \( C \).

\[ E(S_{28}, \text{size} \neq 0) \]
\[ = E(P_{20}) \]

This tells us that in order to traverse Path B the message must have some content and the program counter must point to the start of the path at address 20. The worst-case execution time of Path B is then computed as follows:

\[ W(\text{Path B}) = \sup \{ \tau | pc = 20 \land m(\text{size}) \neq 0 \land 11 \leq \text{size} - \tau \leq 14 \} \]

This tells us that the worst-case execution time of Path B is 14 \( \mu s \), in those cases where the path’s behaviour is well defined. Since this is below the timing constraint 20 that we computed for the functionally equivalent Path A, we can conclude that Path B will always meet the deadline of the high-level program. The implementation’s timing behaviour is correct for this control-flow path.

7. Conclusion

We have defined a semantics for timed program commands and used it to define calculations for traversal conditions and execution-time bounds. We have shown how this approach can be used as a basis for timing analysis of high-level language real-time programs, where
semantic extraction of the “specified” worst-case and best-case execution times is needed to support timing verification of the machine-dependent implementation. We have shown that the techniques can be likewise applied in low-level program analysis with machine languages, where commands may have machine-specific timing bounds defined. In this context, our formal approach can be then used for the derivation of “actual” worst-case and best-case execution times.

The expressive power of our model in terms of nondeterminism and nontermination needs some discussion. Our partial correctness semantics does not allow us to distinguish program states from which either a terminating or nonterminating behaviour is possible from states where only termination is possible. This lack of expressiveness is irrelevant for the computation of worst-case and best-case execution times, since their derivation is relevant only for terminating program executions: in a nondeterministic choice between nontermination and termination our model disregards nontermination, and permits the computation of execution times for the terminating alternative alone. Total correctness semantics would only permit the computation of execution times for “strictly” terminating programs.

The symbolic computation of execution times that we describe in Theorem 5.2 looks tedious and repetitive on paper, but can be automated with techniques from linear programming. This approach permits the approximation of execution times for programs in arbitrary programming languages. A prototype tool using this approach has been implemented in Prolog on the base of linear programming techniques. The tool approximates the supremum (infimum) expressions of Table 5 by transforming the predicates into “linear” predicates and translating the supremum (infimum) computations over the reals into linear optimisation problems. As a result of this, we obtain upper and lower bounds for execution times for arbitrary timed commands in our language [26].

Generally, though, the model is independent of the particular target machine and applies to any programming language with a predicate transformer semantics. In particular, the model provides a sound basis for verification of practical algorithms and tools for worst-case and best-case execution-time prediction.

**Acknowledgements**

This research was conducted as part of ARC Large Grant A49937045, *Effective Real-Time Program Analysis*, and this article was prepared as part of ARC Discovery Grant DP0209722, *Derivation and Timing Analysis of Concurrent Real-Time Software*.

**Appendix A. The predicate space**

Predicates in the space $\text{Pred}$ may have the entire set $\text{Var}$ as free variables. Such a predicate would not permit variable substitution with variables in the variable universe $\text{Var}$ in the usual sense. To avoid pathological cases of this kind we need to make sure that predicates cannot have more than a certain number of free variables. For a given cardinal number $\gamma$, we therefore introduce the set $\text{Pred}_\gamma$, which consists of all predicates $P$ in $\text{Pred}$ such that the cardinality of the set of all free variables of $P$ is not greater than $\gamma$. If $\gamma$ is a limit ordinal, then $\text{Pred}_\gamma$ is closed under infimum (conjunction) and supremum (disjunction) on sets of
predicates from $\text{Pred}_\gamma$, i.e., for predicates $P_i$ from $\text{Pred}_\gamma$, with index $i$ ranging over an index set $A$ of cardinality not greater than $\gamma$, it is the case that $\bigwedge_{i \in A} P_i$ and $\bigvee_{i \in A} P_i$ are predicates in $\text{Pred}_\gamma$. This, in turn, ensures that the definition of nondeterministic choice is well defined.

For a state $\sigma \in \Sigma$, a subset of variables $\mathcal{V} \subseteq \text{Var}$ and a mapping $\mu \in \mathcal{V} \rightarrow \text{Val}$ we define overriding of $\sigma$ by $\mu$, denoted $\sigma \oplus \mu$ by $(\sigma \oplus \mu)(v) \overset{\text{def}}{=} \sigma(v)$ if $v \in \text{Var} \setminus \mathcal{V}$ and by $(\sigma \oplus \mu)(v) \overset{\text{def}}{=} \mu(v)$ if $v \in \mathcal{V}$. A function $f \in \Sigma \rightarrow \text{Val}$ may be independent of a variable $v$ meaning that for every state $\sigma \in \Sigma$ and value $r \in \text{Val}$ the equality $f(\sigma) = f(\sigma \oplus \{v \mapsto r\})$ holds, where $\{v \mapsto r\}$ denotes the mapping of a variable $v$ to a value $r$. The set of all independent variables of $f$ is denoted by $\text{Indep}(f)$. Variable $v$ is called a free variable of $f$ if $v \in \text{Var} \setminus \text{Indep}(f)$.

The term algebra is defined as usual from the set of variables $\text{Var}$ and the set of function symbols $\text{Fun}$ which represent total functions of a certain arity over the value space $\text{Val}$. Substitution of a term $t$ for a variable $v$ in a predicate or function $P$ on $\Sigma$ is defined by $P[t/v](\sigma) \overset{\text{def}}{=} P(\sigma \oplus \{v \mapsto \sigma(t)\})$, where the evaluation of a state $\sigma$ on a term means the canonical extension of $\sigma$ onto the term algebra. By $P[y'/y, z']$ we denote the simultaneous substitution of $y'$ for $y$ and $z'$ for $z$, whereas $P[y'/y][z'/z]$ denotes the substitution of $y'$ for $y$ followed by the substitution of $z'$ for $z$.

The function $\text{Idf}$ gives the set of identifiers used in a command; it is defined in Table A.1.

**Definition A.1 (Supremum).** Let $\mathcal{V} \subseteq \text{Var}$, $B \in \text{Pred}$ and $\theta \in \Sigma \rightarrow (\mathbb{R} \cup \{-\infty, \infty\})$. For $\sigma \in \Sigma$, let the expression $(\sup \{\mathcal{V} | B \bullet \theta\})(\sigma)$ denote the supremum of the set

$$\{\mu \in \mathcal{V} \rightarrow \text{Val} | B(\sigma \oplus \mu) \bullet \theta(\sigma \oplus \mu)\}$$

in $\mathbb{R} \cup \{-\infty, \infty\}$. In addition, for a set $\Omega$ of functions of the same type as $\theta$ above we denote by $(\sup_{\theta \in \Omega} \theta)(\sigma)$ the supremum of the set $\{\theta \in \Omega | true \bullet \theta(\sigma)\}$.

**Appendix B. Basic lemmas and theorems**

**Lemma B.1.** Let $x$ and $y$ be disjoint sets of variables and let $Q$ be a predicate that can only have free primed variables in $x'$. Then, the liberal refinement equivalence $x^{\text{nt}}[Q] \sqsubseteq_{\text{wlp}} x, y^{\text{nt}}[Q \land y = y']$ holds.
Proof. Let $R \in SPred$. Then the following holds:

$$wlp(x^{nt}[Q], R) \equiv \forall x'(Q \Rightarrow R[x'/x])$$

$\equiv$ “Since $y'$ does not occur free in $Q$ and $R$”

$$(\forall x', y'((Q \land y = y') \Rightarrow R[x', y'/x, y]))$$

$\equiv wlp(x, y^{nt}[Q \land y = y'], R). \quad \square$

Lemma B.2. Let $v$ and $x$ denote disjoint sets of variables, then

$$(\forall v : T \bullet x, v^{nt}[Q])C \equiv wlp \ x^{nt}[C \land C[x'/x] \land \exists v, v'(v, v' \in T \land Q)].$$

Proof. Let $R \in SPred$ and let $w \notin Idf((\forall v : T \bullet x, v^{nt}[Q])C)$ and $w \in Indep(R)$. Then the following equivalences hold:

$$wlp((\forall v : T \bullet x, v^{nt}[Q])C, R)$$

$\equiv (\forall v(wlp(x, v^{nt}[Q]) \equiv T \land C[w/v], R[w/v]))[v/w]$

$\equiv (\forall v(\forall x', v'((Q \land v, v' \in T \land C[w/v] \land C[w/v][x'/x])$

$\Rightarrow R[w/v][x'/x]))[v/w]$

$\equiv (\forall x', v'((Q \land v, v' \in T \land C[w/v] \land C[w/v][x'/x])$

$\Rightarrow R[w/v][x'/x]))[v/w]$

$\equiv (\forall x'(C \land C[x'/x] \land \exists v, v'(Q \land v, v' \in T)) \Rightarrow R[x'/x])$

$\equiv wlp(x^{nt}[C \land C[x'/x] \land \exists v, v'(v, v' \in T \land Q), R). \quad \square$

Lemma B.3. $(x^{nt}[Q]; x^{nt}[W]) \equiv wlp \ x^{nt}[\exists v(Q[v/x'] \land W[v/x])].$

Proof. Let $R \in SPred$. Then the following holds:

$$wlp((x^{nt}[Q]; x^{nt}[W]), R) \equiv wlp(x^{nt}[Q], wlp(x^{nt}[W], R))$$

$\equiv \forall x'(Q \Rightarrow (\forall x'(W \Rightarrow R[x'/x]))[x'/x])$

$\equiv $ “Let $v \notin Idf(x^{nt}[Q]) \cup Idf(x^{nt}[W])$

and $v \in Indep(R)”$

$\forall v(Q[v/x']) \Rightarrow (\forall x'(W \Rightarrow R[x'/x]))[v/x])$

$\equiv \forall v(Q[v/x']) \Rightarrow (\forall x'(W[v/x] \Rightarrow R[x'/x]))$

$\equiv \forall x', v((Q[v/x'] \land W[v/x]) \Rightarrow R[x'/x])$

$\equiv \forall x'(\exists v(Q[v/x'] \land W[v/x]) \Rightarrow R[x'/x])$

$\equiv wlp(x^{nt}[\exists v(Q[v/x'] \land W[v/x]), R). \quad \square$

Lemma B.4. $(\forall_{i \in A} x^{nt}[Q_i]) \equiv wlp \ x^{nt}[\forall_{i \in A} Q_i].$
Proof. Let \( R \in SPred \). Then the following holds:

\[
\begin{align*}

wlp\left(x^{.nt}\left[\bigvee_{i \in A} Q_i\right], R\right) & \equiv \forall x'(\left(\bigvee_{i \in A} Q_i \implies R[x'/x]\right)) \\
& \equiv \bigwedge_{i \in A} (Q_i \implies R[x'/x])) \\
& \equiv \bigwedge_{i \in A} (\forall x'(Q_i \implies R[x'/x])) \\
& \equiv wlp\left(\prod_{i \in A} x^{.nt} [Q_i], R\right).
\end{align*}
\]

\[\Box\]

Theorem B.5 (Command reduction). Let \( S \) be a (timed) command, then there is a (timed) specification statement \( S' \) such that \( S \sqsubseteq_{\text{wlp}} S' \) holds.

Proof. This follows from the definition of (timed) commands and Lemmas B.1, B.2, B.3 and B.4. \( \Box \)

Appendix C. Efficient execution-time calculation

For a set of variables \( \mathcal{V} = \{v_1, \ldots, v_n\} \), \( B \in \text{Pred} \), and \( \theta \in \Sigma \to (\mathbb{R} \cup \{-\infty, \infty\}) \), we abbreviate \( \exists v_1, \ldots, v_n B \) by \( \exists \mathcal{V} B \), and \( \{v_1, \ldots, v_n \mid B \bullet \theta\} \) by \( \{\mathcal{V} \mid B \bullet \theta\} \).

Theorem C.1. Let \( \mathcal{V} \subseteq \text{Var} \) and \( \mathcal{W} \subseteq \text{Var} \) be disjoint, \( B \in \text{Pred} \), and \( \theta \in \Sigma \to (\mathbb{R} \cup \{-\infty, \infty\}) \). If \( \mathcal{W} \subseteq \text{Independ}(\theta) \) then the following equality holds:

\[
\sup\{\mathcal{V} \cup \mathcal{W} \mid B \bullet \theta\} = \sup\{\mathcal{V} \mid (\exists \mathcal{W} B) \bullet \theta\}.
\]

Proof. Let \( \sigma \in \Sigma \). Then the following equalities can be easily checked:

\[
\begin{align*}
\text{(sup}\{\mathcal{V} \cup \mathcal{W} \mid B \bullet \theta\})(\sigma) & = \text{supremum}\{\mu \in \mathcal{V} \cup \mathcal{W} \to \text{Val} \mid B(\sigma \oplus \mu) = \text{true} \bullet \theta(\sigma \oplus \mu)\} \\
& = \text{“Since } \mathcal{W} \subseteq \text{Independ}(\theta)\text{”} \\
& \quad \text{supremum}\{\mu' \in \mathcal{V} \to \text{Val} \mid (\exists \mathcal{W} B)(\sigma \oplus \mu') = \text{true} \bullet \theta(\sigma \oplus \mu')\} \\
& = (\text{sup}\{\mathcal{V} \mid (\exists \mathcal{W} B) \bullet \theta\})(\sigma). \quad \Box
\end{align*}
\]

Theorem C.2. Let \( \mathcal{V} \subseteq \text{Var} \), \( A, B \in \text{Pred} \), and \( \theta \in \Sigma \to (\mathbb{R} \cup \{-\infty, \infty\}) \). If \( \mathcal{V} \subseteq \text{Independ}(B) \) then the following entailment relation holds:

\[
B \implies (\text{sup}\{\mathcal{V} \mid A \land B \bullet \theta\} = \text{sup}\{\mathcal{V} \mid A \bullet \theta\}).
\]
Proof. Let $\sigma \in \Sigma$ and assume $B(\sigma)$.

\[
(\sup\{\mathcal{V} \mid A \land B \land \emptyset\})(\sigma)
\]

\[
= \supremum\{\mu \in \mathcal{V} \rightarrow \text{Val} \mid A(\sigma \oplus \mu) \land B(\sigma \oplus \mu) \land \emptyset(\sigma \oplus \mu)\}
\]

\[
= \text{“Since } B(\sigma) \text{ holds and } \mathcal{V} \subseteq \text{Indep}(B)\”
\]

\[
= \supremum\{\mu \in \mathcal{V} \rightarrow \text{Val} \mid A(\sigma \oplus \mu) \land \text{true} \land \emptyset(\sigma \oplus \mu)\}
\]

\[
= (\sup\{\mathcal{V} \mid A \land \emptyset\})(\sigma). \quad \square
\]

References


