The WCET Tool Challenge 2011

Hanxleden, Reinhard von; Holsti, Niklas; Lisper, Björn; Gustafsson, Jan; Islam, Nazrul Mohammad; Ploedereder, Erhard; Fellger, Wolfgang; Gepperth, Sebastian; Krause, Felix; Wilhelm, Reinhard; Bonenfant, Armelle; Casse, Hugues; Michiel, Marianne de; Rochange, Christine; Bünte, Sven; Huber, Benedikt; Kovacs, Laura; Puffitsch, Wolfgang; Zolda, Michael; Zwirchmayr, Jakob; Kästner, Daniel; Wegener, Simon; Kirner, Raimund; Olesen, Mads Christian; Prantl, Adrian; Schoeberl, Martin

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

INSTITUT FÜR INFORMATIK

The WCET Tool Challenge 2011

R. von Hanxleden, N. Holsti, B. Lisper, J. Gustafsson, N. Mohammad Islam, E. Ploedereder, W. Fellger, S. Gepperth, F. Krause, R. Wilhelm, A. Bonenfant, H. Cassé, M. de Michiel, C. Rochange, S. Bünte, B. Huber, L. Kovács, W. Puffitsch, M. Zolda, J. Zwirchmayr, D. Kästner, S. Wegener, R. Kirner, M. C. Olesen, A. Prantl, and M. Schoeberl

Bericht Nr. 1215

October 2012

ISSN 2192-6247

CHRISTIAN-ALBRECHTS-UNIVERSITÄT

ZU KIEL

Institut für Informatik der
Christian-Albrechts-Universität zu Kiel
Olshausenstr. 40
D – 24098 Kiel

The WCET Tool Challenge 2011

R. von Hanxleden, N. Holsti, B. Lisper, J. Gustafsson, N. Mohammad Islam, E. Ploedereder, W. Fellger, S. Gepperth, F. Krause, R. Wilhelm, A. Bonenfant, H. Cassé, M. de Michiel, C. Rochange, S. Bünte, B. Huber, L. Kovács, W. Puffitsch, M. Zolda, J. Zwirchmayr, D. Kästner, S. Wegener, R. Kirner, M. C. Olesen, A. Prantl, and M. Schoeberl

Bericht Nr. 1215
October 2012
ISSN 2192-6247

Contact e-mail: rvh@informatik.uni-kiel.de

The WCET Tool Challenge 2011*

REINHARD VON HANXLEDEN, Christian-Albrechts-Universität zu Kiel
NIKLAS HOLSTI, Tidorum Ltd
BJÖRN LISPER and JAN GUSTAFSSON and NAZRUL MOHAMMAD ISLAM, Mälardalen University
ERHARD PLOEDEREDER and WOLFGANG FELLGER and SEBASTIAN GEPPERTH and FELIX KRAUSE, University of Stuttgart
REINHARD WILHELM, Universität des Saarlandes
ARMELLE BONENFANT and HUGUES CASSÉ and MARIANNE DE MICHIEL and CHRISTINE ROCHANGE, IRIT - CNRS, Université de Toulouse
SVEN BÜNTE and BENEDIKT HUBER and LAURA KOVÁCS and WOLFGANG PUFFITSCH and MICHAEL ZOLDA and JAKOB ZWIRCHMAYR, Technical University Vienna
DANIEL KÄSTNER and SIMON WEGENER, AbsInt Angewandte Informatik GmbH
RAIMUND KIRNER, University of Hertfordshire
MADS CHRISTIAN OLESEN, Aalborg University
ADRIAN PRANTL, Lawrence Livermore National Laboratory
MARTIN SCHOEBERL, Technical University of Denmark

*This work is supported by the ARTIST DESIGN Network of Excellence.

Author's addresses: R. von Hanxleden, Department of Computer Science, Christian-Albrechts-Universität zu Kiel, Olshausenstr. 40, 24098 Kiel, Germany; N. Holsti, Tidorum Ltd, Tiirasaarentie 32, FI-00200 Helsinki, Finland; B. Lisper, J. Gustafsson, N. M. Islam, School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden; E. Ploedereder, W. Fellger, S. Gepperth, F. Krause, Institute of Software Technology (ISTE), University of Stuttgart, Universitätsstr. 38, 71229 Stuttgart, Germany; R. Wilhelm, FR. 6.2 - Computer Science, Universität des Saarlandes, PO-Box 15 11 50, 66041 Saarbrücken, Germany; A. Bonenfant, H. CassÉ, M. de Michiel, C. Rochange, IRIT - CNRS, Université de Toulouse, France; S. Bünte, B. Huber, L. Kovács, W. Puffitsch, M. Zolda, J. Zwirchmayr, Faculty of Informatics, Technical University Vienna, 1040 Vienna; D. Kästner, S. Wegener, AbsInt Angewandte Informatik GmbH, Science Park 1, 66123 Saarbrücken, Germany; R. Kirner, Compiler Technology and Computer Architecture Group, University of Hertfordshire, Hatfield, Hertfordshire, AL10 9AB, UK; M. C. Olesen, Department of Computer Science, Aalborg University, Selma Lagerlöfs Vej 300, 9220 Aalborg, Denmark; A. Prantl, Lawrence Livermore National Laboratory, P.O. Box 808, Livermore, CA 94551, USA; M. Schoeberl, Department of Informatics and Mathematical Modeling, Technical University of Denmark, Asmussens Alle, DTU - Building 305, 2800 Lyngby, Denmark.

Abstract

Following the successful WCET Tool Challenges in 2006 and 2008, the third event in this series was organized in 2011, again with support from the ARTIST DESIGN Network of Excellence. Following the practice established in the previous Challenges, the WCET Tool Challenge 2011 (WCC'11) defined two kinds of problems to be solved by the Challenge participants with their tools, *WCET problems*, which ask for bounds on the execution time, and *flow-analysis problems*, which ask for bounds on the number of times certain parts of the code can be executed. The benchmarks to be used in WCC'11 were debie1, PapaBench, and an industrial-strength application from the automotive domain provided by Daimler AG. Two default execution platforms were suggested to the participants, the ARM7 as "simple target" and the MPC5553/5554 as a "complex target," but participants were free to use other platforms as well. Ten tools participated in WCC'11: aiT, Astrée, Bound-T, FORTAS, METAMOC, OTAWA, SWEET, TimeWeaver, TuBound and WCA.

1 Introduction

The chief characteristic of (hard) real-time computing is the requirement to complete the computation by a given deadline. The execution time usually depends on the input data and the architecture's state.

1.1 The WCET Problem Statement and Existing Approaches

It is important to find the worst-case execution time (WCET) and verify that it is short enough to meet the deadlines in all cases.

Several methods and tools for WCET analysis have been developed. Some tools are commercially available. The survey by Wilhelm et al. (2008) is a good introduction to these methods and tools. Some tools use pure static analysis of the program; other tools combine static analysis with dynamic measurements of the execution times of program parts. Unlike most applications of program analysis, WCET tools must analyse the *machine code*, not (only) the source code. This means that the analysis depends on the target processor, so a WCET tool typically comes in several versions, one for each supported target processor or even for each target system with a particular set of caches and memory interfaces. Some parts of the machine-code analysis may also depend on the compiler that generates the machine code. For example, the analysis of control-flow in switch-case statements may be sensitive to the compiler's idiomatic use of jumps via tables of addresses.

In general, WCET tools use simplifying approximations and so determine an *upper bound* on the WCET, not the *true* WCET. The pessimism, that is the difference between the true WCET and the upper bound, may be large in some cases. For most real, non-trivial programs a fully automatic

WCET analysis is not (yet) possible which means that manual *annotations* or *assertions* are needed to define essential information such as loop iteration bounds. The need for such annotations, and the form in which the annotations are written, depends on both the WCET tool and on the target program to be analysed.

1.2 The WCET Tool Challenge: Aims and History

As the term "Challenge" suggests, the aim is not to find a "winning" tool but to challenge the participating tools with common benchmark problems and to enable cross-tool comparisons along several dimensions, including the degree of analysis automation (of control-flow analysis, in particular), the expressiveness and usability of the annotation mechanism, and the precision and safety of the computed WCET bounds. Through the Challenge, tool developers can demonstrate what their tools can do, and potential users of these tools can compare the features of different tools.

Jan Gustafsson of the Mälardalen Real-Time Centre organized the first WCET Tool Challenge in 2006, using the Mälardalen benchmark collection (Gustafsson, Betts, Ermedahl, and Lisper 2010) and the PapaBench benchmark (Nemer et al. 2006), with participation from five tools (aiT, Bound-T, SWEET, MTime, and Chronos). Lili Tan of the University of Duisburg-Essen did the evaluation of the tools on these benchmarks and reported about the results (Gustafsson 2006; Gustafsson 2007) and later in STTT (Tan 2009).

The second WCET Tool Challenge was organized in 2008 (WCC'08). Results were presented at the 8th International Workshop on Worst-Case Execution Time (WCET) Analysis (Holsti et al. 2008). Two of the WCC'06 participants (Bound-T and MTime) as well as four new tools (OTAWA, RapiTime, TuBound and wcc) participated in WCC'08. The second Challenge differed from the first in that it suggested a common execution platform (the ARM7 LPC2138) and also defined pure flow-analysis problems. It included less benchmarks (5 instead of 17), but increased the number of analysis problems.

1.3 Contributions and Outline

The third WCET Tool Challenge was organized in 2011 (WCC'11[1]) and is the subject of this report. As a first overview, Table 1 lists the tools participating in the Challenge and indicates which target processors each participant has addressed for WCC'11; most tools support other target processors, too.

[1] `http://www.mrtc.mdh.se/projects/WCC/` — this web page links to the wiki of the WCC'11 as well as to the previous WCC editions.

Tool	Description in Section	Source-code flow analysis	ARM7 (Sec. A.1)	MPC5554 (Sec. A.2)	Other target processors
aiT	2.1		+	+	
Astrée	2.2	+			
Bound-T	2.3		+		
FORTAS	2.4	+			TC1796 (Sec. A.3)
METAMOC	2.5				
OTAWA	2.6	+	+	+	
SWEET	2.7	+			
TimeWeaver	2.8			+	
TuBound	2.9	+			C167 (Sec. A.4)
WCA	2.10				JOP (Sec. A.5)

Table 1: Participating tools and target processors used in WCC'11.

This report combines contributions from the WCC'11 participants and is edited by the WCC'11 steering group, some of whom are also WCC'11 participants. In Sec. 2, the most substantial section of this report, the participants in turn describe their tools and the experiences in participating in the Challenge. The overall results are reported in Sec. 3. In addition to the tool authors who tested their tools on the debie1 and PapaBench benchmarks, a group of students of the University of Stuttgart, led by Erhard Ploedereder, tried some of the tools on a proprietary benchmark supplied by Daimler AG; they report their experience in Sec. 4. The paper concludes in Sec. 5. The target architectures are described in the appendix A.

It should be noted that not only the Challenge itself, but also this report adopts much from the previous edition, including both structure and content. Specifically, the WCET problem statement, the descriptions of the ARM processor and the debie1 benchmark, and the presentation of the types of analysis problems are largely quoted from the WCC'08 report (Holsti et al. 2008). Maintaining most of the report structure may facilitate tracing the development of the Challenge and the participating tools.

1.4 The Benchmarks

Thanks to Daimler, we could from the beginning count on an industrial-size, real-world benchmark to be included in WCC'11, see Sec. 1.4.3. However, it was also clear rather early that this benchmark would not be suitable for all analysis tools. To broaden the tool base, and to also be attractive to participants of previous Challenges, we decided to reuse two benchmarks, the PapaBench already used in WCC'06 (Sec. 1.4.2), and the debie1 benchmark introduced in WCC'08 (see Sec. 1.4.1).

1.4.1 The debie1 benchmark

The debie1 (First Standard Space Debris Monitoring Instrument, European Space Agency[2]) benchmark is based on the on-board software of the DEBIE-1 satellite instrument for measuring impacts of small space debris and micro-meteoroids. The software is written in C, originally for the 8051 processor architecture, specifically an 80C32 processor that is the core of the the Data Processing Unit (DPU) in DEBIE-1. The software consists of six tasks (threads). The main function is interrupt-driven: when an impact is recorded by a sensor unit, the interrupt handler starts a chain of actions that read the electrical and mechanical sensors, classify the impact according to certain quantitative criteria, and store the data in the SRAM memory. These actions have hard real-time deadlines that come from the electrical characteristics (hold time) of the sensors. Some of the actions are done in the interrupt handler, some in an ordinary task that is activated by a message from the interrupt handler. Two other interrupts drive communication tasks: telecommand reception and telemetry transmission. A periodic housekeeping task monitors the system by measuring voltages and temperatures and checking them against normal limits, and by other checks. The DEBIE-1 software and its WCET analysis with Bound-T were described at the DASIA'2000 conference (Holsti, Långbacka, and Saarinen 2000).

The real DEBIE-1 flight software was converted into the debie1 benchmark by removing the proprietary real-time kernel and the low-level peripheral interface code and substituting a test harness that simulates some of those functions. Moreover, a suite of tests was created in the form of a test driver function. The benchmark program is single-threaded, not concurrent; the test driver simulates concurrency by invoking thread main functions in a specific order. The DEBIE-1 application functions, the test harness, and the test driver are linked into the same executable. This work was done at Tidorum Ltd by Niklas Holsti with ARTIST2 funding.

Space Systems Finland Ltd (SSF), the developer of the DEBIE-1 software, provides the software for use as a WCET benchmark under specific Terms of Use that do not allow fully open distribution. Copies of the software can be requested from Tidorum[3]. SSF has authorized Tidorum to distribute the software for such purposes.

1.4.2 The PapaBench Benchmark

PapaBench (Nemer, Cassé, Sainrat, Bahsoun, and Michiel 2006) is a WCET benchmark derived from the Paparazzi UAV controller. This controller has been developed in the ENAC school in Toulouse and targets low-cost UAV,

[2] `http://gate.etamax.de/edid/publicaccess/debie1.php`
[3] `http://www.tidorum.fi/`

that is, model airplane embedding a microprocessor.

Basically, the UAV is made of several actuators (motor, flaps, etc) and a very light set of sensors including a GPS (connected by a serial port) and an infrared sensor to control slope. The system may be controlled from ground using a classical wireless link or may fly in an autonomous mode performing a pre-programmed mission. In this case, the wireless descending link is only used to transfer flight log or video if the payload is composed of a little camera.

In its original configuration, the computing hardware was composed of two ATMEL AVR microprocessors communicating by a SPI link. The first one, fbw (fly-by-wire), was responsible for the control of actuators and sensors and for the stabilization of the flight. It was also used to perform commands emitted by the wireless link. The second microprocessor, autopilot, was a bit more powerful and was concerned with the realization of the mission, that is, the choice of the flight plan. The system has several emergency modes activated according to the whole system state. In a first mode, it tries to return to its "home" base. In another one, it tries to save the integrity of the model plane by ensuring a minimal landing drive. And in a very bad case, it puts the actuators in a configuration ensuring it will simply plane gracefully in the hope it may land without breaking anything.

To perform a flight, the first task is to program a flight plan and to generate automatically a piece of code included in the embedded software system. Then, the full system is compiled and composed of two binary programs: fbw and autopilot. In the next step, the programs are transferred to the controller and the plane is launched (by hand) and the controller starts to drive the plane. If all is ok, the flight plan ends with the model plane landing at its starting point.

1.4.3 The Daimler benchmark

The benchmark is part of a control system for trucks that deals with, among others, collision detection. The code is compiled for the MPC 5553 architecture using the WindRiver Diab compiler. The target processor does not have any external memory. VLE instructions are not used.

Due in part to circumstances described in section 4.2, the ultimate choice of WCET questions was directed at four entry points below the task level of different types:

- An interrupt handler `INTERR`

  It is a simple interrupt handler that only calls one function and does not include any loops.

- An initialization routine `INIT`: This is a second simple entry point that sets some variables, does not call any functions and has no loops.

- Two calculation routines `CALC1` and `CALC2`: These routines execute moderately complex numeric calculations. They include some loops and static function calls.

- A complete task of the embedded system `TASK`: This is a typical task of an embedded system; it is the body of an endless loop that executes some subtasks and then suspends itself until it needs to run again.

1.5 The Analysis Problems

For each WCC benchmark, a number of analysis problems or questions are defined for the participants to analyse and answer. There are two kinds of problems: WCET-analysis problems and flow-analysis problems. Flow-analysis problems can be answered by tools that focus on flow-analysis (for example SWEET) but that do not have the "low-level" analysis for computing WCET bounds. Flow-analysis problems can also show differences in the flow-analyses of different WCET tools, and this may explain differences in the WCET bounds computed by the tools.

A typical WCET-analysis problem asks for bounds on the WCET of a specific subprogram within the benchmark program (including the execution of other subprograms called from this subprogram). For example, problem 4a-T1 for the debie1 benchmark asks for the WCET of the Handle_Telecommand function when the variable input data satisfy some specific constraints.

A typical flow-analysis problem asks for bounds on the number of times the benchmark program executes a certain statement, or a certain set of statements, within one execution of a root subprogram. For example, problem 4a-F1 for the debie1 benchmark asks how many calls of the macro `SET_DATA_BYTE` can be executed within one execution of the function Handle-Tele-command, under the same input-data constraints as in the WCET-analysis problem 4a-T1. By further requiring the analysis to assume that the execution time of `SET_DATA_BYTE` is arbitrarily large we make it possible for pure WCET-analysis tools to answer this flow-analysis question, since this assumption forces the worst-case path to include the maximum number of `SET_DATA_BYTE` calls; all alternative paths have a smaller execution time.

2 Tools and Experience

An overview of the tools and target processors used in WCC'11 was given in Table 1. As indicated there, five out of ten tools do flow analysis on the source-code level. This means that their flow-analysis results could in principle be compared in source-code terms. For example, on the source-code level we can talk about iteration bounds for specific loops, which is not possible on the machine-code level because of code optimizations.

On the ARM7, aiT, Bound-T, OTAWA used the gcc ARM 3.4.1 for PapaBench, and the gcc-if07 for debie1. TuBound used the gcc-c16x for the C167. aiT and TimeWeaver used the powerpc-eabi-gcc (Sourcery G++ Lite 2010.09-56) 4.5.1 for the MPC5554. FORTAS used the hightec-tricore-gcc-3.4.5 for the TC1796.

In the following, each tool is briefly described, followed by a report on the experience and results gained by participating in WCC'11. The descriptions are written by the developers of the tool, edited only for uniform formatting.

2.1 aiT (written by S. Wegener and D. Kästner)

AbsInt's aiT[4] is a timing verification tool. Static WCET analysis is used to compute a safe upper bound of the actual WCET of a task. Its target processors range from simple architectures like the ARM7TDMI to highly complex architectures like the PowerPC 7448.

The main input of aiT is the binary executable, from which the control-flow graph is reconstructed. No code modification is required. On the control-flow graph, several static analyses take place to compute the execution time of each instruction. A global path analysis is used afterwards to compute the task's overall WCET bound. Manual annotations can be used to express known control-flow facts or values of registers and memory cells. aiT has been successfully used for timing verification in the avionics, aeronautics and automotive industries (e. g. (Souyris et al. 2005; NASA Engineering and Safety Center 2011)).

aiT already supported the proposed common target architectures. Thus nothing had to be changed to analyze the benchmarks. Nevertheless, both the control-flow reconstruction part of aiT as well as the loop analysis part have been extended to reduce the amount of annotations that must be manually added to perform the analyses of the benchmarks.

2.1.1 Analysis of the debie1 benchmark

Both the MPC5554 version and the ARM7 version have been analyzed.

A WCET bound could be computed for each problem. For the T2 problems concerning the maximal interrupt blocking times, we are assuming for any function containing the interrupt enabling/disabling macro that the entire function is executed with disabled interrupts. This had to be done because the macros DISABLE_INTERRUPT_MASTER and ENABLE_INTERRUPT_MASTER were defined as no-ops and thus not visible in the binary. Only little overestimation is introduced by this simplification since most routines called the macros directly at the beginning and at the end. As an exceptional case, the routine "RecordEvent" enables interrupts, calls "FindMinQualityRecord" and then disables the interrupts again. Here, the

[4] `http://www.absint.com/ait/`

WCET contribution of "FindMinQualityRecord" has been subtracted from the WCET contribution of "RecordEvent" to get the execution time of the interrupt-disabled region.

Most loop bounds were derived automatically by aiT. For those loops where this was not the case loop bound annotations have been manually added. The input constraints as defined in the WCET Tool Challenge's wiki[5] have been used to write annotations for the analyses. All input constraints except one could be transformed to annotations. The one exception is problem 2c for ARM7. Here, the compiler transformed an if-then-else construct into conditionally executable code. Although aiT analyzes conditionally executable code, there is at the moment no possibility to annotate the state of the condition flags.

The annotations provided to aiT can be found in the wiki of the 2011 WCET Tool Challenge. Also all the flow questions were answered. However, the invocation counts are computed only for the worst-case path. Due to this, the answers of problem 6d, question F1 differ between the ARM7 and the MPC5554. On the latter, "SetSensorUnitOff" is not on the critical path and thus the invocation count is zero (instead of eight on the ARM7).

2.1.2 Analysis of the PapaBench benchmark

Only the ARM7 code in RAM version has been analyzed. A bound[6] could be computed for each problem. One problem during the analysis was that the fly-by-wire executable contains debug information which could not be read by aiT or GNU objdump. Fortunately, the benchmark's creator was able to send a file which contained the mapping between source code lines and binary code addresses. With the help of this file, we could also answer the flow question of problem F1b. Another problem were the loops in the software floating point library. This floating point library is not used by any of our commercial customers and no loop bound annotations were available.

aiT was only able to derive some loop bounds, but not all. To derive the remaining bounds by hand/brain would have required more effort than we were willing to invest. Therefore, we simply assumed 99 iterations for the actual division loop.

Of the flow questions, only those regarding feasible or unfeasible code have been answered. The rest of the questions concerned the bounds of angle normalisation loops for which aiT did not automatically find loop bounds. We simply annotated them to iterate once. Our annotations can be found in the wiki of the 2011 WCET Tool Challenge.

[5] http://www.mrtc.mdh.se/projects/WCC/2011/doku.php?id=bench:debie1, as of May 5, 2011

[6] The correctness of this bound depends on the correctness of our loop bound assumptions.

2.1.3 Comments on the Daimler benchmark

Comparing the results in Table 6 (Sec. 4.3) for the aiT OTAWA-like MPC5554 configuration and OTAWA MPC5554 for the small code snippets `INTERR` and `INIT`, we see a rather high difference of a factor of about 2.

AbsInt found the OTAWA MPC5554 results to be surprisingly low in some cases and assumed that OTAWA underestimates the WCET. Without access to the Daimler code, we used another executable and used our MPC5554 evaluation board to produce a NEXUS trace for the entry point of a given function in the processor configuration supported by OTAWA. This trace shows an execution time of around 451 cycles, while the OTAWA tool only predicts 320 cycles. We therefore assume that there is a difference in the CPU modeling of aiT and OTAWA and the results are not comparable. Unfortunately, it was not possible to get actual hardware measurements from Daimler for the entry points we used.

2.2 Astrée (written by S. Wegener and D. Kästner)

Astrée[7] (Kästner et al. 2010) is a verification tool to prove the absence of runtime errors in embedded C code compliant to the C99 standard. Examples of runtime errors which are handled by Astrée include division by zero, out-of-bounds array indexing, and erroneous pointer accesses. Moreover, Astrée can be used to prove that user-defined assertions are not violated. As an experimental feature, Astrée can export loop bound annotations and function pointer target annotations for aiT.

Astrée is not directly targeted at WCET analysis. However, the information it computes can be used to help the WCET analysis. For the debie1 benchmark, Astrée has been used to derive flow facts (like loop bounds and function pointer targets) from the C source code.

2.2.1 Analysis of the debie1 benchmark

Astrée is not directly targeted on flow analysis. However, we were interested how well Astrée can be used to retrieve flow information useful for WCET analysis.

An experimental feature has been added to Astrée to produce loop bound annotations and function pointer target annotations for aiT. To count routine invocations, for each routine of interest, an own static integer variable had been added. These variables are incremented by one for each routine invocation. Astrée's value analysis is then used to derive an interval for these variables. Answers were produced for all flow problems.

The following assumptions have been used during the analysis: (1) Only the tasks of interest have been analyzed, but no initialization routines, be-

[7] `http://www.absint.com/astree/`

cause the problem specification stated that any task may run between the invocation of the particular task and its initialization tasks. Thus all possible values have been assumed for those variables that were not initialized inside the analyzed tasks. (2) For those variables where some input constraints were given in the problem description the constraints have been used to narrow down the value range of these variables.

The analysis of the debie1 benchmark showed that in principle, Astrée can be used to compute the flow information needed for WCET analysis.

2.3 Bound-T (written by N. Holsti)

Bound-T is a WCET analysis tool that uses static analysis of machine code to compute WCET bounds and (optionally) stack-usage bounds. Starting from the entry point of the specified root subprogram Bound-T constructs the control-flow and call graphs by fetching and decoding binary instructions from the executable file. Bound-T models the integer computations as transfer relations described by Presburger arithmetic formulas and then analyses the transfer relations to identify loop induction variables and loop bounds and to resolve dynamic branches. Some infeasible paths may also be detected. Various simpler analyses such as constant propagation and copy propagation are applied before the powerful but costly Presburger models. Bound-T is focused on microcontrollers with predictable timing. Caches and other very dynamic hardware components are not considered. The WCET is calculated with the Implicit Path Enumeration technique, applied to each subprogram separately. Bound-T is commercially distributed and supported by Tidorum Ltd.

2.3.1 Bound-T's Participation in this Challenge

Of the target processors suggested for the 2011 WCET Challenge, Bound-T supports only the ARM7. Participation was thus limited to the benchmarks available for the ARM7: debie1 and PapaBench. Both benchmarks have been used in earlier Challenges. For the 2011 Challenge the debie1 analysis problems were slightly changed, based on participant feedback from the 2008 Challenge, so the Bound-T annotations had to be updated correspondingly. PapaBench was used in the 2006 Challenge, but not in 2008 when the "analysis problem" structure was introduced, so the PapaBench analysis problems were new. However, many low-level annotations from the 2006 Challenge could be reused.

2.3.2 Problems with Benchmarks

The capabilities of Bound-T have evolved only a little since the 2008 Challenge, so all of the difficulties with debie1 in the 2008 Challenge are still

present, for example the inability to find and analyse the WCET of interrupt-disabled code regions, as required by the debie1 analysis problems 5a-T2 and others. Many of the constraints and assumptions in the debie1 analysis problems cannot be expressed as such in the Bound-T annotation language, but must be translated into different kinds of annotations that have the same effect on the analysis. For example, there is no way to assert that a variable does not have a specific value, as required by the debie1 analysis problem 2a. This translation requires study of the benchmark source code and is not always easy.

PapaBench created new problems, some of which were quite different from the debie1 problems. In PapaBench, almost all loops aim to normalize floating-point variables, representing angles, to some basic "unwrapped" range, for example 0 to 360 degrees. The loops do this by repeatedly adding or subtracting a full circle until the basic range is reached. Bound-T does not attempt to find bounds for loops where termination depends on floating-point conditions, so loop bounds had to be found manually. This meant finding bounds on the value of the angle variable on entry to the normalisation loops. This was tolerably easy for some cases, but too hard in other cases, for which the loop bounds were guessed.

The PapaBench analysis problem A5 asks for the WCET of a part of a C function. Bound-T does not have a general "point-to-point" analysis capability, but in this case the interesting part is the tail end of the function, so Bound-T was told to analyse the "function" starting at the first instruction in the interesting part, as if this instruction were the entry point of a function, and go on in the normal way to the return instruction.

2.3.3 Conclusions for Bound-T

The 2011 Challenge did not reveal any new problems or inspire new ideas for improving Bound-T. However, it was a useful reminder about the problems with translating constraints from the conceptual, application-oriented level to concrete, code-oriented annotations. This is a gap that should be filled, but filling it may need new ideas for representing really high-level constraints in WCET analysis.

2.4 FORTAS (written by S. Bünte, M. Zolda, and R. Kirner)

FORTAS (the *FORmal Timing Analysis Suite*) derives WCET estimates of software tasks running on embedded real-time systems. The FORTAS tool suite is based on a hybrid approach that combines execution time measurements with static program analysis techniques and follows the general principles of *measurement-based timing analysis* (MBTA) (Wenzel, Kirner, Rieder, and Puschner 2008).

The FORTAS tool suite extends the classical workflow of MBTA, which

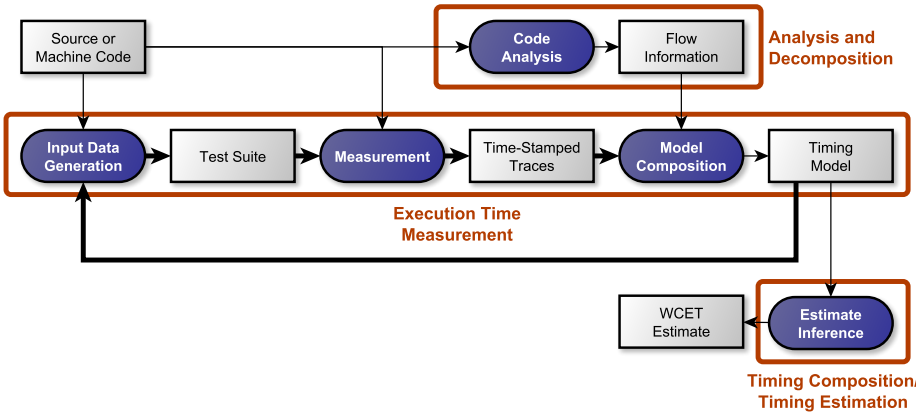

Figure 1: Workflow of measurement-based timing analysis in FORTAS

consists of the three stages *analysis and decomposition*, *execution time measurement*, and *timing estimation/composition*, by introducing feedback-driven input data generation, as illustrated by Figure 1. Unlike many other approaches, the FORTAS tool suite does not devise one ultimate WCET estimate—it rather produces an ongoing sequence of progressively more precise estimates. In particular, the FORTAS tool suite uses feedback-driven input data generation to reduce optimism in the timing model (Bünte, Zolda, Tautschnig, and Kirner 2011; Buente, Zolda, and Kirner 2011). In practice, the estimate converges quickly to a sufficiently stable value, such that the analysis can be finished. To limit the pessimism during timing estimation, the FORTAS tool suite uses context-sensitive IPET (Zolda, Bünte, and Kirner 2011).

2.4.1 Porting the Benchmarks

We ported PapaBench to the TC1796 (described in Sec. A.3) and analyzed problems `A1`, `A2A`, `F1a`, `F1b`, and `F2`.

- We removed the scheduler and analyzed each target function of the respective benchmark problem in isolation. Code that is not needed for a problem is omitted. Analyzing the whole source code in its original version is not feasible with our input data generation technique.
- We annotated trigonometrical functions from our TC1796 `math.h` with *assume statements* of the model checker CBMC to restrict the domain of function arguments. We did this to partly re-incorporate context information that had been lost by removing the scheduler.
- We added start-up code that initializes the processor. The code manipulates TriCore-specific registers to set the CPU clock to a frequency of 150MHz.

- We changed the benchmark to emulate certain accesses to memory registers by global variables. For example, the call of the macro `SpiIsSelected()` was substituted by a read access to a global variable `spi_is_selected`.

- We expanded the preprocessor macros and moved some C expressions and statements to dedicated source code lines, in order to get a canonical version that is interpreted consistently among all FORTAS tools. For the same reason we made short-cut evaluation in decisions and conditional expressions explicit, i.e., we translated such conditionals to semantically equivalent cascades of `if`-statements.

- We converted loops, so that iteration bounds are easily found by CBMC.

- We removed `static` and `inline` declarations without changing the program semantics. Also, we substituted `typedef` directives with equivalent types that do not incorporate any `typedef`. The reason for this modification is that these features are not supported by our prototype.

The transformed versions of PapaBench can be downloaded from our website[8].

2.4.2 Analysis

With our prototype implementation we can analyze ISO C code. We use HighTec's GCC version 3.4.5 to compile the source code for our target processor, the TriCore 1796. We then executed the program on the target platform and captured cycle-accurately time-stamped execution traces using a *Lauterbach LA-7690 PowerTrace* device that is connected to the target system via the processor's *On-Chip Debug Support* (OCDS) *Level 2* debugging interface.

Internally, our tools work on a CFG representation of the software under analysis. Loop bounds and other flow facts are currently provided by the user. In the current setting we turned optimization off when compiling the benchmark sources. This is needed in the current implementation stage of the prototype implementation. But this will not be needed in the future, as we have recently shown within the research project SECCO[9] that we can achieve quite high optimization while still maintaining preservation of structural code coverage criteria.

We automatically generate suitable input data using a model-checking based method [Holzer, Schallhart, Tautschnig, and Veith 2008; 2009] that

[8] `http://www.fortastic.net/benchmarks_wcc_2011.zip`
[9] `http://pan.vmars.tuwien.ac.at/secco/`

has been implemented as the FSHELL[10] tool. FSHELL itself is based on the C Bounded Model Checker (CBMC) version 3.8 (Clarke, Kroening, and Lerda 2004). The input to FSHELL is a test suite specification, expressed in the *FShell Query Language* (FQL) (Holzer, Schallhart, Tautschnig, and Veith 2010).

2.4.3 Problems and Solutions

We encountered several limitations of our analysis tool, most of which are due to the nature of our prototypical implementation: we had to change the benchmarks manually (see above) in order to make them work with the FORTAS tool suite, which took far more time than we expected. However, those issues can be resolved given sufficient engineering resources to resolve those prototypical deficiencies.

However, some limitations are specific to our analysis approach: the reason why we cannot analyze problems A2b and A3-A6 is due to limitations of our input data generation techniques. Our version of CBMC utilizes an SMT solver that cannot find models for the respective problems efficiently. We suspect the combination of floating point variables and multiplication operations to be the source of the problem. This seems to point at a need for complementary generation methods for input data.

2.4.4 Comments on the WCET Tool Challenge

First, our research benefits from the extended pool of benchmarks. Second, some of the encountered limitations will drive us both in terms of tool engineering and in addressing the problem of input data generation in our future research.

Unfortunately, our prototype implementation is not compliant to any of the target processors that are officially supported by the challenge. Also, we did not have the resources available to add another target system to our tool. Retargeting an MBTA tool to a new target platform requires considerably less effort than in the case of a static WCET analysis tool, but still needs some effort to set up the tool chain.

2.5 METAMOC (written by M. C. Olesen)

METAMOC (Dalsgaard et al. 2010) analyses WCET problems by converting the CFG of a program into a timed automata model, which is combined with models of the execution platform (pipeline, caches). The combined model is then model checked using the UPPAAL model checker, asking for the maximal value the cycle counter can attain, which is then the WCET estimate. No automated flow analysis is implemented, so all flow facts and

[10] `http://code.forsyte.de/fshell`

loop bounds have to be manually annotated, either in the C source code, or by modifying the resulting model. Non-determinism is used to explore all branches, and can therefore also be used in the annotations, if there are uncertainties. Of course, the less precise the annotations the more possibilities the model checker has to explore, and too little precision results in the model checker running out of memory.

2.5.1 Experience

The WCET Challenge was the first time we applied our tool to a real-world benchmark. As such, we were not able to solve many of the problems. The main problem we encountered in applying METAMOC was getting annotations of a good enough quality. Particularly the floating point routines compiled in by GCC are of crucial importance: they are called very frequently so therefore the annotations need to be of high quality (to limit the possible paths through the function), but on the other hand the routines are highly optimized so therefore hard to analyse.

2.6 OTAWA (written by A. Bonenfant, H. Cassé, M. de Michiel, and C. Rochange)

OTAWA (Ballabriga, Cassé, Rochange, and Sainrat 2011) is a library dedicated to the development of WCET analyzers. It includes a range of facilities such as:

- loaders
  - to load the binary code to be analyzed. Several ISAs are supported: PowerPC, ARM, TriCore, Sparc, HCS12. New binary loaders can be generated with the help of our GLISS tool (Ratsiambahotra, Cassé, and Sainrat 2009).
  - to load a description of the flow facts (loop bounds, targets of indirect branches, imposed branch directions). For complex flow facts, the description can be supplemented with a set of hand-written constraints to be added to the ILP formulation (IPET (Li and Malik 1995)).
  - to load a description of the target hardware (processor, memory hierarchy, memory map, etc.). Only generic architectures can be described that way: fort specific targets the user needs to write specific analyses where needed.
- annotation facilities (called *properties*) that make it possible to annotate any object (instruction, basic block, etc.) with any kind of value. They are used to store the results of the successive analyses.

- code processors that use already-computed annotations and produce new ones. Built-in code processors include a CFG builder, a CFG virtualizer, loop dominance analyzers, support for abstract interpretation, hardware analyzers (pipeline, caches, branch predictor), and a WCET calculator based on the IPET method (with the help of the `lp_solve` tool).

The library comes with a set of built-in tools that check for absolutely-required flow facts, dump the CFG in various formats (e. g. dot), compute a WCET following an input script that describes the specific analyses to be applied, etc. These tools are also available in an Eclipse plugin.

OTAWA is open-source software available under the LGPL licence[11].

2.6.1 Problems and solutions

Both the recommended targets, namely the PowerPC MPC5554 and the ARM LPC2138 have been modeled in OTAWA. However, we discovered that the PowerPC version of the debie1 benchmark includes VLE instructions which are not supported by OTAWA so far. Then we decided to focus on the ARM target.

The problems we have encountered are all related to flow facts. Some are inherent to the code of the benchmarks, others come from the questions we had to answer.

General difficulties. To compute loop bounds automatically, we use the oRange (Michiel, Bonenfant, Cassé, and Sainrat 2008) companion tool developed in our group. It works on the source code. Unfortunately, oRange was not able to determine all the bounds: for some of the problems, the source code of some functions was missing (e. g. debie1 5a, PapaBench F1a); the increment of some of the loops (e. g. in debie1 6b) could not be computed. In such cases, we determined the bounds by hand, with success for most of them. This is a fastidious and error-prone work. For functions (e. g. `memcpy`) from the `glibc`, we considered the source codes found on the GNU web site.

For some functions, we have found several possible sets of loop bounds (e. g. the bounds for *loop*1 and *loop*2 are either x and y, or x' and y' respectively). This cannot be directly specified to OTAWA. In such cases, we have added appropriate constraints on the sum of iterations of both loops.

Difficulties related to the Challenge questions. Several questions required considering specific switch cases. Our simple flow facts description language does not support this kind of annotations. We added hand-written constraints to the integer linear program. It seems fastidious but in practice

[11] `www.otawa.fr`

it is quite easy thanks to an efficient CFG displayer that shows various information like basic block numbers, branch directions, related source code lines, etc.

Problem 3b for debie1 raised the difficulty mentioned above since it implied that one of two identical loops ends after one iteration instead of processing to the end value. We had to hand-write additional constraints.

2.7 SWEET (written by J. Gustafsson and N. M. Islam)

SWEET (Swedish WCET Analysis Tool) is a WCET analysis research tool from MDH. It has a standard WCET tool architecture, consisting of a program flow analysis, a low-level analysis, and a WCET estimate calculation.

SWEET analyzes the intermediate format ALF (Gustafsson et al. 2009). ALF can represent code on source-, intermediate- and binary level through relatively direct translations. Given a code format, SWEET can perform a WCET analysis for it if there is a translator into ALF. Currently, two translators exist: a translator from C to ALF from TU Vienna, and an experimental translator from PowerPC binaries. The first translator enables SWEET to perform source-level WCET analysis. This translator has been used in the WCET Challenge.

The current focus of SWEET is on automatic program flow analysis, where constraints on the program flow are detected. SWEET's program flow analysis is called *abstract execution* (Gustafsson, Ermedahl, Sandberg, and Lisper 2006). This analysis is *input-sensitive*, meaning that it can take restrictions on program input values into account to produce tighter flow constraints. Abstract execution can compute a wide ranges of program flow constraints, ranging from simple loop bounds to complex infeasible path constraints. The constraints can be context-sensitive, to allow for greater precision.

SWEET can handle ISO C programs including pointers, and unstructured code. It has a large set of options for fine-tuning the analysis. It has an annotation language, where the user can provide additional information that the automatic analysis for some reason fails to derive.

Since SWEET does not support the target processors in the WCET Challenge 2011, we have only performed source-level program flow analysis. We restricted the analysis to PapaBench; debie1 was excluded due to lack of time, and the Daimler code was excluded since we anticipated problems for the students performing the analysis on the Daimler code to use our tool. In particular, the C to ALF translator is hard to install due to its many dependencies to different software packages. We also know by experience that production source code for embedded systems can pose many problems for source-level analysis tools, since such code often stretches the C standard (Lisper et al. 2010).

2.7.1 The flow analysis problems

We were able to obtain answers to all six PapaBench flow analysis problems. In particular, SWEET managed to find bounds also for the floating-point controlled loops in problems A1, and A2a. Due to the input-sensitivity of SWEET's flow analysis, we were able to derive bounds for these that are conditional on certain input values. These bounds are more precise than bounds that have to be valid for all possible input value combinations. The conditions, in the form of input ranges for certain input variables, were found by a search running SWEET with different input ranges for these variables. Interestingly, for problem A2a our analysis also found a possible division by zero if the input variable `estimator_hspeed_mod` is zero. If this variable indeed can assume this value, then there is a potential bug in PapaBench.

For some problems we had to tweak the code, or take some other measures, to make the analysis go through. For problem A3, we had to remove the "inline" keyword at three places since our C to ALF translator did not accept this use of the keyword. The code for problem F1b contains an infinite loop: we had to patch the code to make this loop terminate to perform the analysis.

At some places in the PapaBench code, absolute addresses are referenced. Such references are problematic when analyzing unlinked source code, since potentially any program variable can be allocated to that address when the code is linked. Thus a safe analysis must assume that the absolute address can be aliased with any program variable, and this is indeed what SWEET assumes by default. However, this will typically lead to a very imprecise analysis. To remedy this, we equipped SWEET with a mode where it assumes that all absolute addresses are distinct from all unallocated program variables. This is often a reasonable assumption, since absolute addresses typically are used to access I/O ports and similar which are distinct from data memory. In this mode, the analysis also assumes that absolute addresses always hold the abstract TOP value (no information about its possible value), since the value of input ports and similar can be altered from outside the program. In all but very unusual situations, an analysis resting on these assumptions should be safe.

2.7.2 Conclusions, and lessons learned

SWEET was able to solve all six program flow analysis problems posed for PapaBench automatically. Notably, these problems include loops that are controlled by floating-point variables. We had to tweak the source code at some places to make all analyses go through: however, these tweaks were necessitated by current limitations in translator and analysis tool that are not of fundamental nature, and fixing them should be a mere matter of engineering.

2.8 TimeWeaver (written by S. Wegener and D. Kästner)

AbsInt's TimeWeaver is a measurement-based timing estimation tool. It can be used for any processor with NEXUS-like tracing facilities[12], i.e. with hardware support for non-invasive tracing mechanisms. TimeWeaver's main focus is not timing verification but exploring the worst-case timing behavior on actual hardware and identifying hot-spots for program optimizations.

The main design goal for TimeWeaver was simplicity. After specifying the set of input traces and the analysis starting point, TimeWeaver is able to compute a WCET estimate in a fully automatic way. All the needed information is taken from the measurements. At the current point of time, no additional knowledge can be added by annotations. If for example a loop has at most five iterations in the traces, but the assumption is that the particular loop has a bound of ten iterations, the analysis is only able to use the bound of five. Unfortunately, this hampers the comparability of TimeWeaver with other WCET tools, but on the other hand, it eases the use of TimeWeaver.

To compute a WCET estimate, an ILP is constructed from the traces which represents the dynamic control-flow graph as observed by the measurements. Loop bounds and time stamps are also extracted from the traces.

2.8.1 Adapting TimeWeaver to the proposed common target architectures

As TimeWeaver works on NEXUS traces, only the MPC5554 was considered as target. For this processor, a prototype already existed. This prototype has been extended to handle incomplete traces. Moreover, the handling of routines with multiple exits has been improved.

2.8.2 Analysis of the debie1 benchmark

The debie1 benchmark was the only one which was analyzed with TimeWeaver because it was the only one available for the MPC5554. Since TimeWeaver is a measurement-based tool, the quality of the results depends heavily on the quality of the input traces. Unfortunately, the measurement solution used to get the traces showed some unforeseen problems (see next section). No comparable results were therefore computed by TimeWeaver.

2.8.3 Trace generation problems

The first problem was the lack of automation support of the rather old tracing equipment available at AbsInt. Producing several thousand traces[13]

[12] `http://www.nexus5001.org/`

[13] According to Niklas Holsti, the test harness triggers about 52500 individual task invocations.

for each task invocation manually one by one would have been a huge effort and was not considered as a practical option. Instead, we tried to trace the harness part as a whole.

This approach uncovered two other problems. First, the distinction between the various subquestions was not possible with the large traces because the NEXUS traces contain only instruction addresses and timestamps. Thus, only estimates for the entire tasks could be computed, without taking the input constraints into account. Second, the trace buffer of the used measurement equipment is of only limited size. Thus sometimes the traces ended prematurely and no full path coverage was achieved.

2.8.4 Comments on the WCET Tool Challenge

For the next incarnations of the Challenge, we believe that having a standard set of measurements would be a tremendous advantage. Then, all measurement-based tools could use the same input, thus enabling more room for comparison. Moreover, having traces of the worst-case paths would also ease the comparison between the actual WCET and the computed estimates. Last but not least, this would prevent the participants from suffering from the same problems we had.

2.9 TuBound (written by Adrian Prantl and Jakob Zwirchmayr)

TuBound is a research prototype WCET analysis and program development tool-chain (Prantl, Knoop, Schordan, and Triska 2008) from Vienna University of Technology, built on top of libraries, frameworks and tools for program analysis and transformation. Flow information is acquired and annotated (either supplied by the user or inferred by an analyzer or a software model checker) at source code level. TuBound's loop bound analysis component was recently extended by SMT reasoning to rewrite multi-path loops into single-path ones. Additionally, certain classes of single-path loops are translated into a set of recurrence relations over program variables, which are then solved by a pattern-based recurrence solving algorithm. The extension is denoted r-TuBound and described in more detail by Knoop et al. (2011b, 2011a).

The gathered flow information is conjointly transformed within the development tool chain. The transformed annotations are further used by the WCET analyzer to calculate the WCET.

TuBound combines a C/C++ source-to-source transformer (the ROSE compiler framework), static analysis libraries (SATIrE, TERMITE), used to implement a forward-directed data flow interval analysis, a points-to analysis and a loop bound analysis, a WCET-aware C compiler (based on GNU C compiler 2.7.2.1 ported to the Infineon C167 architecture with added WCET

analysis functionality), and a static WCET analysis tool. The WCET analysis tool currently integrated into the TuBound tool-chain is Calc_wcet_167, a static WCET analysis tool that supports the Infineon C167 as target processor. Further details about TuBound can be found in (Prantl, Schordan, and Knoop 2008; Prantl, Knoop, Schordan, and Triska 2008).

2.9.1 TuBound—Target Architecture

TuBound currently only supports the Infineon C167 architecture, described in Sec. A.4).

2.9.2 TuBound Problems with Benchmarks

General In some cases it was not possible to annotate the input constraints because there is no support for them in TuBound. For example, TuBound supports neither path annotations specifying "the first run" (or in general the xth run), nor constraints that specify that "function f is executed once before g." Additionally, the interval analysis does not support arbitrary user supplied value annotations. Some of the input constraints can nevertheless be annotated manually. For the cases where the input constraints could not be annotated fully, we report the worst-case result. Therefore, for example, when the WCET of "the first run" of a function is asked for, we calculate the WCET of the function and use it as result. If there are constrained inputs that we cannot model, we again compute the (general) WCET of this function and report it as an over-approximation of the WCET of the run in question.

Another difficulty stems from the supplied assembler code: we cannot perform WCET calculation for the assembler code, because we do not support the target architecture. Therefore we could not, for example, find out the WCET of interrupt routine `__vector_10`.

Another feature TuBound is still missing is floating point support: interval analysis does not consider float values; those are used, for example, in parts of the PapaBench inputs.

Tool Challenge The upper loop bound problems in PapaBench all involved floats, which we do not handle in our interval analysis, even though in principle the loops could be bound by our loop analyzers.

The evaluation of the tool on industry benchmarks at Daimler showed the need for a shippable binary version of TuBound, as the compilation and installation effort is quite high.

Additionally, there are portability issues in TuBound that need to be addressed (e. g. hard-coded paths). These issues are not of utmost importance, as TuBound is still a research prototype. Nevertheless it would be beneficial to allow outside evaluation by non-experts/developers.

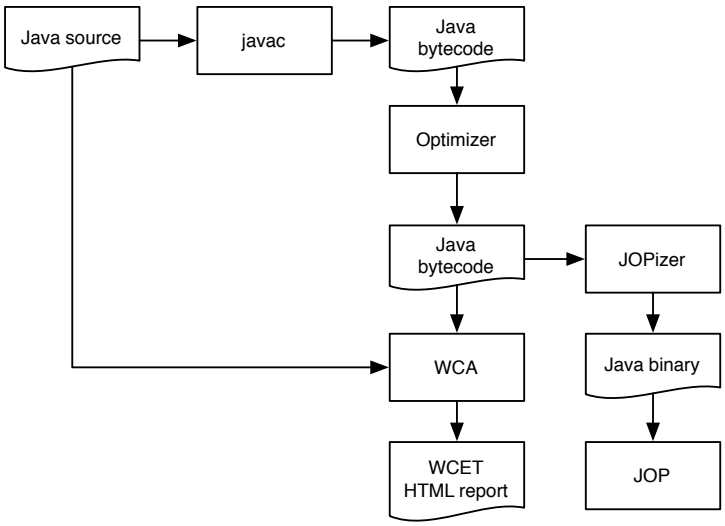

Figure 2: Tools and compilation, optimization, analysis, and build flow for JOP.

2.10 WCA (written by B. Huber, W. Puffitsch and M. Schoeberl)

The WCA tool (Schoeberl, Puffitsch, Pedersen, and Huber 2010) from Vienna University of Technology and DTU is a static WCET analysis tool for processors executing Java bytecode, currently only supporting JOP (Schoeberl 2008). The input to the analysis tool are Java class files, along with information on the processor configuration. The latter consists of hardware parameters, such as cache sizes and memory access timings, and of the microcode assembler code for each bytecode.

Figure 2 gives an overview of the tools and the build and analysis flow. Java source, with optional loop bound annotations, is compiled with a standard Java compiler to Java bytecode. The optional optimizer uses bytecode as input and produces bytecode. The bytecode is the input for the WCA tool that produces reports in HTML. WCA also reads the Java source to extract annotations. The bytecode is also the input for the tool JOPizer to generate a linked executable, which is downloaded to JOP.

For the high-level path analysis, bytecode has several advantages compared to machine code. Most type information is still present in bytecode, even automated decompilation is feasible. In particular, it is easy to automatically obtain control flow graphs from bytecode. The possible targets for indirect branches (switch) are specified in the class file. Instead of indirect function calls, bytecode solely relies on dynamic method dispatch.

Determining the methods possibly executed due to a virtual invocation amounts to determining the dynamic type of the receiving object. WCA

includes a data flow analysis (DFA) to determine precise dynamic types of objects, which is also used to prune the call graph. Additionally, the DFA computes bounds on the range of values. This information is used for a simple loop bound analysis, which makes it unnecessary to manually analyze and annotate many loops rates. Manual loop bounds may be provided at the source code level. The annotation language supports bounds relative to outer loops and symbolic expressions. In particular, it is possible to refer to Java constants in loop bound expressions, which reduces the maintenance burden considerably.

The pipeline analysis for JOP is relatively straightforward. One distinguishing feature of WCA is that it derives a symbolic formula for the worst-case execution time of bytecode instructions automatically. To this end, the microcode sequence executed for a bytecode is inspected. The analysis composes a formula which takes explicitly hidden memory latencies and method cache accesses into account.

WCA also includes a static analysis for JOP's method cache. It implements a scope-based persistence analysis for the N-block method cache with FIFO replacement. This analysis inspects program fragments, and tries to prove that, within one fragment, at most N cache blocks are accessed. If this is indeed the case, method cache costs only need to be accounted for once for a method accessed within the fragment. This is encoded in the IPET formulation, using a standard technique adding cache miss and cache hit variables.

Although WCA is a command line tool, it produces annotated listings of Java code, which can be used to inspect the worst-case path. As we maintain relatively precise bytecode to source code line mappings, this can be done on the Java source code.

The combination of WCA and JOP is a little bit different from the other tools participating in the Challenge as we support Java instead of C. Therefore, we had to port the benchmarks to Java. Furthermore, the different languages and the different execution platform make is problematic to compare WCA with the other tools.

2.10.1 Porting the Benchmarks to Java

While we could reuse the Java port of Papabench from Kalibera et al. (2010), the debie1 benchmark was ported by ourselves. Unfortunately, the port of Papabench is incomplete. As we did not want to deviate too far from the publicly available version of the benchmark, we fixed only a few minor issues, but left the general implementation of the benchmark unchanged. One notable change in the implementation was the use of scoped memory to enable dynamic memory allocation while avoiding garbage collection. Due to the incompleteness of the benchmark, we were only able to answer a few questions posed by the Challenge. In order to provide a more complete

picture, we include the analyzed and observed WCETs of the benchmark's tasks in Table 3.

debie1 was ported as far as necessary to properly execute the test cases provided in the harness. However, some functionality was omitted as it would not have been possible to test the respective code properly.

During porting, we encountered a few advantages and disadvantages of Java. In C, structs are laid out flat in memory and can be accessed byte for byte through a pointer. In Java, accessing an object byte for byte requires manual mapping of byte indices to fields, which is considerably more expensive. A related issue are accesses to multidimensional arrays. While in C it is possible to use a unidimensional index to access elements in such an array, this is not possible in Java. For accesses to a multidimensional array in Java, it is necessary to compute the correct index for each dimension, which requires a division and remainder operations. If strength reduction is not possible, this introduces severe overheads.

Java has a clear concept for modularization. While it is still possible to write poorly modularized code, the object orientation of Java serves as gentle reminder to programmers. Also, being able to control the visibility of fields encourages clean interfaces. Some of the arguments above are against Java in real-time systems due to the considerable overhead inherited by an object-oriented language. However, it should be noted that Java with its strong typing and runtime checks is a safer language than C and therefore, in the opinion of the authors, an interesting choice for safety-critical applications.

2.10.2 Problems and Insights

debie1 The main problem in the analysis of debie1 (in particular Problem 1 and Problem 3) is that methods tend to be very long. We usually assume that in safety-critical code, methods are kept short, as recommended by safety-critical programming guidelines (e. g., (Holzmann 2006)). In our "literal" port of the debie1 benchmark to Java, there are many very long methods along with very large switch statements. First, the method cache of JOP can be rather inefficient for very long methods. Secondly, our cache analysis uses rather coarse-grained scopes (methods only) for persistence analysis, and therefore delivers poor results for Problem 1 and Problem 3. From the analysis point of view, considering subgraphs as persistency scopes would considerably improve the analysis. Another attractive option is to automatically refactor large methods into smaller ones. A related problem is the use of switch statements to implement what usually would be realized using dynamic dispatch in Java. This leads to very large methods, which severely impact the method cache performance, even in the average case. Again, refactoring to more idiomatic code (Command Pattern (Gamma, Helm, Johnson, and Vlissides 1994)) would resolve this problem.

We replaced all the preprocessor-based configuration in the original de-

Problem	all-miss	all-hit	WCET	Measured
(1)	19111	12719	17717	6977
(2a-2c)	9960	7385	9104	6601
(3a-3c)	158549	120561	132353	67666
(4a-4d)	32150	24419	26863	24652
(5a-5b)	1661×10^3	1371×10^3	1382×10^3	1289×10^3

Table 2: Analysis results for jDebie problems (in clock cycles).

bie1 code by methods of a Java interface, which abstracts the actual hardware. In order to eliminate the resulting efficiency penalty, it is necessary to have an optimizer to remove this indirection once the configuration of the hardware platform is fixed. An optimizer for Java bytecode is currently under development, which includes method inlining. As this optimizer is still under development, the execution times for the interrupt handling routines are very high.

On the positive side, we used the chance to improve our annotation language, which now supports arbitrary expressions involving Java constants. For example, the annotation for the checksum calculation is

```
// @WCA loop <= union(CHECK_SIZE, 1 + CODE_MEMORY_END
// - MAX_CHECKSUM_COUNT * CHECK_SIZE)
```

where `CHECK_SIZE`, etc. are Java constants defined in the code.

The results for debie1 are given in Table 2. To show the effectiveness of the method cache analysis we also show analysis results with the assumption of all misses in the method cache and all hits in the method cache (in the second and third columns). The WCET analysis result must lie between these extremes.

For Problem 6, we did not find meaningful flow constraints, and thus failed to determine a reasonable WCET bound. We did not work on the flow analysis subproblems, lacking support for artificial flow constraints, and only analyzed the worst-case path for each problem. Although we prefer to minimize the use of manual annotations, after working on the debie1 problem set we believe an interactive tool to explore different paths would be a valuable addition to WCA.

Papabench Papabench was relatively straightforward to analyze, even though our value analysis could not cope with the multi-threaded code. In fact, only two (symbolic) loop bounds had to be annotated in the application code. However, the use of floating-point operations proved problematic. On the one hand several loops with non-obvious bounds had to be annotated in the software implementations of these operations, on the other hand the

Task	all-miss	all-hit	WCET	Measured
AltitudeControl	33078	27978	29054	23667
ClimbControl	139987	120938	126515	105926
RadioControl	69216	60198	64266	2444
Stabilization	168261	150349	156974	131910
LinkFBWSend		21 (empty)		0
Reporting		21 (empty)		0
Navigation		cyclic CFG		3057905
CheckMega128Values	9710	8618	9710	9417
SendDataToAutopilot	11692	10104	11574	393
TestPPM	4633	3341	4629	610
CheckFailsafe		cyclic CFG		515

Table 3: Analysis results for jPapabench tasks (in clock cycles).

resulting execution times were less than satisfying, both in analysis and measurements. Although we were able to correctly bound the execution times for the floating-point operations, we do not think that such code is suitable for embedded applications. Figure 3 shows the analysis results and execution time measurements.

3 Results

The full set of results is too large to be presented here; please refer to the Wiki. Table 4 shows the number of analysis problems for each WCC'11 benchmark, the number of flow-analysis and WCET-analysis questions to be answered, and the number of questions answered by each participating tool. If a tool answers the same question for several target processors, it still counts as only one answer.

For the three tools that analyzed the simple processor target (ARM7), Table 5 lists the specific results. As can be seen, most deviations are less than 50%. However, there are notable exceptions that probably deserve further investigation.

4 The Daimler Experiment (written by E. Ploedereder, F. Krause, S. Gepperth, and W. Fellger)

WCC'11 as described so far had the producers of applicable tools bring their intimate knowledge to bear in processing previously available benchmarks. In the Daimler experiment, students of the University of Stuttgart applied the tools to proprietary industrial software (see Sec. 1.4.3). The students

Benchmark	**debie1**		**PapaBench**		**Daimler**
Type of question	Flow	WCET	Flow	WCET	WCET
Number of questions	15	22	6	11	4
aiT	15	22	3	11	4
Astrée	15				
Bound-T	14	18	5	11	
Fortas				5	
METAMOC					
OTAWA	8	15	5	11	4
SWEET			6		
TimeWeaver		6			
TuBound	15	18	1	10	
WCA		13		11	

Table 4: Number of posed and answered analysis problems in WCC'11.

had no prior knowledge of either the tools or the analyzed software. They were remotely supported by the tool providers and had access to Daimler employees knowledgeable about the analyzed system.

4.1 The Tools

The target architecture MPC5553 is supported by few of the tools participating in the WCC'11. The experiment was conducted with AbsInt's aiT and with OTAWA, as these tools are the only ones that support the target architecture. It should be noted that OTAWA only supports the MPC 5554 architecture, which is one reason for the somewhat surprising divergence in the results obtained by the two tools. As a third tool, TuBound had registered for the experiment but we did not succeed in its on-site installation.

4.2 Experiences with the Two Tools

The analyzed software contains fault branches trapping in infinite loops. Obviously, this cannot be accommodated in a WCET calculation. The fault branches needed to be filtered out to obtain meaningful results.

With aiT the respective branches and function calls leading to infinite loops could be excluded from the WCET calculation. With OTAWA, unfortunately no approach could be identified to achieve such exclusion. Encountering such an infinite loop sometimes led OTAWA itself into an infinite loop, requiring a forced termination. The entry point `TASK` was a case in point. Hence it could not be included in the comparison of WCET results.

Apart from this, OTAWA frequently terminated with a segmentation fault when analyzing the Daimler code. It also terminated the Eclipse IDE

debie1	**Estimated clock cycles**		
	aiT	Bound-T	OTAWA
1	342	333	332
2a	100	93	139
2b	144	143	139
2c	144	138	139
3a	2664	2692	4101
3b	11404	11402	23829
3c	11664	11662	27117
4a	2352	2343	522460
4b	215	214	210
4c	196	187	195
4d	199	190	730
5a T1	4154	5223	5329
5a T2	172		42
5b T1	38798	39825	55883
5b T2	180		42
6a T1	22203	22765	
6a T2	98		
6b	23100	23741	
6c	40143	42285	
6d	24184	24254	
6e T1	1101107	372148	
6e T2	158		

Papa-	**Estimated clock cycles**		
Bench	aiT	Bound-T	OTAWA
A1	1716	1660	1358
A2a	27785	31699	32735
A2b	31482	37181	38112
A3 T1	3404	3849	1119
A3 T2	8938	10484	9863
A4	4182	5986	5953
A5	5435	5131	4782
A6	12051	17378	17422
F1a	4207	7914	7824
F1b	45	43	40
F2	102	100	102

Table 5: Results for WCET analysis questions for the ARM7. The *estimated clock cycles* refer to the results reported by aiT, Bound-T, and OTAWA.

if the plugin was used. Despite best efforts from both Daimler and OTAWA supporters, these problems could not be resolved in time. A suspected cause might be related to what OTAWA calls "unresolved controls," potential branch instructions in the code that cannot be automatically resolved. They occurred very frequently in the Daimler code, and we suspect that a "wrong" choice was taken from the available substitutes.

Absint's aiT was pretty straightforward to use and did not cause any major problems that could not be dealt with quickly; in particular, it could deal with almost all branches without further interaction. We checked the resulting call graphs for overestimation of loop bounds - which were mostly automatically computed - but they were all reasonable.

OTAWA itself does not compute loop boundaries, so they needed to be set statically for every loop. It should be noted that OTAWA is combined with an external tool called "oRange" for this job which we did not get to experiment with because of the general stability issues.

4.3 Results

The comparative results consist of three data sets, two for aiT and one for OTAWA. These data sets presented in Table 6 are:

- aiT configured for the real hardware. This configuration yields proper WCET results for the hardware the code is compiled for.
- aiT configured for comparison to OTAWA results. The hardware configuration is changed to assume the same parameters OTAWA uses in its MPC 5554 configuration.
- OTAWA with MPC5554 configuration. As OTAWA does not support the exact hardware configuration the code is written for, this configuration is as close as the experiment could get to the real hardware.

OTAWA offers predefined configuration "scripts" with very few options, while aiT presents an almost overwhelming range of settings. For aiT, we made use of the option to initialize the CPU settings from actual CPU status registers for the *real hardware configuration*.

The loop boundaries used for OTAWA were slightly overestimated compared to the ones used for aiT, as each loop count can only be set globally, not per call to the containing function. The context sensitivity of loop bound estimation in aiT is particularly noticeable in `CALC2`, the only entry point for which the OTAWA result is higher than the corresponding aiT result.

4.4 Conclusion on the Daimler experiment

In order to arrive at comparable numbers, we reran aiT with a CPU configuration approximating the configuration used by OTAWA to get any-

Entry point	aiT		OTAWA
	Compiled hardware configuration	OTAWA-like configuration	
INTERR	524	204	113
INIT	1055	494	218
CALC1	2124	830	722
CALC2	16507	6218	7991

Table 6: WCET computation results for the Daimler code experiment.

where near comparable results. While these were in fact significantly closer, OTAWA still tended to give lower numbers than aiT.

In searching for causes of the remaining divergence, we traced the estimates down to the individual basic blocks. Even at this level, the estimates by OTAWA remained consistently lower, which makes it very likely that there are hidden differences in the CPU modeling of the two tools that account for the spread in numbers. The OTAWA support concurred in this being a likely cause.

Unfortunately, no actual hardware or faithful emulator was available to the experiment in order to measure actual performance and compare it to the predictions in order to determine how close the predictions came to reality and whether any numbers were underestimations for the actual hardware. AbsInt had hardware available and undertook a test of this hypothesis. AbsInt reports on the results in Sec. 2.1.3. This report supported our impression that it is very important to ensure a precise match of the detailed hardware description to the actual hardware in arriving at meaningful WCET answers that reflect reality or that allow a comparision of numbers obtained by different tools.

5 Conclusions

One of the goals formulated in the conclusions of the last Challenge, WCC'08 (Holsti et al. 2008), was "to motivate the 2006 participants to rejoin the Challenge, without losing the new 2008 participants." We have adopted this goal, and wanted to provide a setting that would be attractive to as many participants as possible, irrespective of whether or not they had participated in earlier Challenges. Thus, we aimed for a sense of continuity of the Challenge, to allow previous participants to re-use some of their previous investments, and for a sense of openness, to allow new participants to join the Challenge even if they could not comply with the suggested targets (ARM7 or MPC) or programming language (C). We also followed the suggestion of

the WCC'08 report to include PapaBench, already used in WCC'06 but not in WCC'08, again in WCC'11. We are thus happy to have had ten participating tools, up from five in 2006 and six in 2008. The ten 2011 participants include three 2006 participants (aiT, Bound-T, and SWEET), three 2008 participants (Bound-T again, OTAWA, and TuBound) and five first-time participants (Astrée, FORTAS, METAMOC, TimeWeaver, and WCA).

One price of the openness is reduced comparability of results. Ultimately, WCET analysis is about numbers, which should supply a natural metric to compare the tools. However, the presence of numerical results may also give a false sense of objectivity, and may tempt to compare apples with oranges. All participants provided numerical results, but these involved a range of target architectures, tool chains, and manual annotation effort. For future editions of the benchmark, it would be nice if more convergence could be reached here, at least for a "simple" processor/benchmark setting.

Furthermore, while we are convinced that all participants do their best to produce safe results (ie., to not underestimate the WCET), the absence of validated "true" WCETs also leaves the possibility of results that are (unintentionally) too good to be true. It is not clear how to circumvent this problem in practice. Then again, this is an issue that affects not only the WCC, but the whole WCET analysis discipline. Furthermore, the WCC might help the tool designers to uncover potential points for improvements in their tools (not only with respect to tightness, but also with respect to safety), which is just the point of the Challenge. Ideally, future editions of the Challenge would not only include safe estimates that strive for tightness and bound the true WCET from above (where lower is better), but would also include maximal established measurements that bound the true WCET from below (where higher is better). This still would not prove the safety of the WCET estimates, but could serve as a minimal consistency check.

One of the assets of WCC'11, the availability of an industrial code, also posed one of the organizational challenges. It turned out non-trivial to align the non-disclosure requirements and architectural constraints of the code with the capabilities of the participating tools. It would be nice if a future Challenge would have more participants for an industrial-size benchmark and the "complex processor" category.

The report on the last Challenge concluded (Holsti et al. 2008): "The WCC'08 organizers suggest that the Challenge should be defined as a continuous process, allowing the addition of benchmarks, participants, and analysis results at any time, punctuated by an annual deadline. At the annual deadline, a snapshot of the results is taken and becomes the result of the Challenge for that year." So far, this goal has turned out a bit too ambitious, but we hope with this Challenge to have made another step towards maturity of the Challenge and, more importantly, the involved tools. We certainly hope that there will be another WCC'1X Challenge, and hope that it will find a good balance between continuing established practice and

adding new elements.

Acknowledgments

From the Steering Committee, we wish to conclude by thanking all participants who actively contributed to the success of the Challenge from its very beginning, when they helped to define the setting, to the end, when they delivered their reports on time. We also thank the organizers of the previous Challenges, upon whose work we could build.

References

ARM (1995, August). Advanced RISC Machines, ARM7DMI Data Sheet. Document Number ARM DDI 0029E, Issue E.

Ballabriga, C., H. Cassé, C. Rochange, and P. Sainrat (2011). OTAWA: An Open Toolbox for Adaptive WCET Analysis. In S. Min, R. Pettit, P. Puschner, and T. Ungerer (Eds.), *Software Technologies for Embedded and Ubiquitous Systems*, Volume 6399 of *Lecture Notes in Computer Science*, pp. 35–46. Berlin / Heidelberg: Springer.

Buente, S., M. Zolda, and R. Kirner (2011, June). Let's get less optimistic in measurement-based timing analysis. In *Proc. 6th IEEE International Symposium on Industrial Embedded Systems (SIES'11)*, Västerås, Sweden. IEEE. To appear.

Bünte, S., M. Zolda, M. Tautschnig, and R. Kirner (2011, March). Improving the confidence in measurement-based timing analysis. In *Proc. 14th IEEE International Symposium on Object/Component/Service-oriented Real-time Distributed Computing (ISORC'11)*, Newport Beach, CA, USA. IEEE.

Clarke, E., D. Kroening, and F. Lerda (2004). A tool for checking ANSI-C programs. In K. Jensen and A. Podelski (Eds.), *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2004)*, Volume 2988 of *Lecture Notes in Computer Science*, Barcelona, Spain, pp. 168–176. Springer.

Dalsgaard, A. E., M. C. Olesen, M. Toft, R. R. Hansen, and K. G. Larsen (2010). METAMOC: Modular Execution Time Analysis using Model Checking. In B. Lisper (Ed.), *10th International Workshop on Worst-Case Execution Time Analysis (WCET 2010)*, Volume 15 of *OpenAccess Series in Informatics (OASIcs)*, Dagstuhl, Germany, pp. 113–123. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. The printed version of the WCET'10 proceedings are published by OCG (www.ocg.at) - ISBN 978-3-85403-268-7.

Gamma, E., R. Helm, R. Johnson, and J. M. Vlissides (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Boston, MA, USA: Addison Wesley Professional.

Gustafsson, J. (2006). The worst case execution time tool challenge 2006. In *Proceedings of the Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation*, Washington, DC, USA, pp. 233–240. IEEE Computer Society.

Gustafsson, J. (2007, January). WCET Challenge 2006. Technical Report ISSN 1404-3041 ISRN MDH-MRTC-206/2007-1-SE, Mälardalen University.

Gustafsson, J., A. Betts, A. Ermedahl, and B. Lisper (2010, July). The Mälardalen WCET benchmarks — past, present and future. In B. Lisper (Ed.), *Proc. 10th International Workshop on Worst-Case Execution Time Analysis (WCET'2010)*, Brussels, Belgium, pp. 137–147. OCG.

Gustafsson, J., A. Ermedahl, B. Lisper, C. Sandberg, and L. Källberg (2009, June). ALF – a language for WCET flow analysis. In N. Holsti (Ed.), *Proc. 9th International Workshop on Worst-Case Execution Time Analysis (WCET'2009)*, Dublin, Ireland, pp. 1–11. OCG.

Gustafsson, J., A. Ermedahl, C. Sandberg, and B. Lisper (2006, December). Automatic derivation of loop bounds and infeasible paths for WCET analysis using abstract execution. In *Proc. 27th IEEE Real-Time Systems Symposium (RTSS'06)*, Rio de Janeiro, Brazil. IEEE.

Holsti, N., J. Gustafsson, G. Bernat, C. Ballabriga, A. Bonenfant, R. Bourgade, H. Cassé, D. Cordes, A. Kadlec, R. Kirner, J. Knoop, P. Lokuciejewski, N. Merriam, M. de Michiel, A. Prantl, B. Rieder, C. Rochange, P. Sainrat, and M. Schordan (2008). WCET Tool Challenge 2008: Report. In R. Kirner (Ed.), *8th Intl. Workshop on Worst-Case Execution Time (WCET) Analysis*, Dagstuhl, Germany. Schloss Dagstuhl—Leibniz-Zentrum fuer Informatik, Germany. also published in print by Austrian Computer Society (OCG) under ISBN 978-3-85403-237-3.

Holsti, N., T. Långbacka, and S. Saarinen (2000, September). Using a Worst-Case Execution Time Tool for Real-Time Verification of the Debie Software. In B. Schürmann (Ed.), *Data Systems in Aerospace (DASIA 2000)*, Volume 457, Montreal, Canada. ESA Publications Division.

Holzer, A., C. Schallhart, M. Tautschnig, and H. Veith (2008, July). Fshell: Systematic test case generation for dynamic analysis and measurement. In *Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008)*, Volume 5123 of *Lec-*

ture Notes in Computer Science, Princeton, NJ, USA, pp. 209–213. Springer.

Holzer, A., C. Schallhart, M. Tautschnig, and H. Veith (2009, January). Query-driven program testing. In N. D. Jones and M. Müller-Olm (Eds.), *Proceedings of the Tenth International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2009)*, Volume 5403 of *Lecture Notes in Computer Science*, Savannah, GA, USA, pp. 151–166. Springer.

Holzer, A., C. Schallhart, M. Tautschnig, and H. Veith (2010, September). How did you specify your test suite? In *Proceedings of the 25th IEEE/ACM International Conference on Automated Software Engineering (ASE 2010)*, Antwerp, Belgium. ACM.

Holzmann, G. (2006, June). The power of 10: rules for developing safety-critical code. *Computer 39*(6), 95–99.

Huber, B., W. Puffitsch, and M. Schoeberl (2011). Worst-case execution time analysis driven object cache design.

Infineon (2003). *TriCore Compiler Writer's Guide*. `http://www.infineon.com`: Infineon.

Infineon (2005a). C167CR/SR Data Sheet. `http://infineon.com`.

Infineon (2005b). *TriBoard TC1796 Hardware Manual*. `http://www.infineon.com`: Infineon.

Infineon (2007). *TC1796 User's Manual V2.0*. `http://www.infineon.com`: Infineon.

Kalibera, T., P. Parizek, M. Malohlava, and M. Schoeberl (2010). Exhaustive testing of safety critical Java. In *Proceedings of the 8th International Workshop on Java Technologies for Real-time and Embedded Systems (JTRES 2010)*, New York, NY, USA, pp. 164–174. ACM.

Kästner, D., S. Wilhelm, S. Nenova, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, and X. Rival (2010, May). Astrée: Proving the absence of runtime errors. In *Embedded Real Time Software and Systems (ERTS^2 2010)*, pp. 1–9. `http://www.di.ens.fr/~mine/publi/kastner-al-erts10.pdf`.

Knoop, J., L. Kovacs, and J. Zwirchmayr (2011a, July 5,). An Evaluation of WCET Analysis using Symbolic Loop Bounds. In *Proceedings of the 11th International Workshop on Worst-Case Execution Time Analysis (WCET 2011)*, Porto, Portugal. To appear.

Knoop, J., L. Kovacs, and J. Zwirchmayr (2011b, June 27–July 1,). Symbolic Loop Bound Computation for WCET Analysis. In *Proceedings of the 8th International Andrei Ershov Memorial*

Conference—Perspectives of System Informatics (PSI 2011), Akademgorodok/Novosibirsk, Russia. Springer. To appear.

Li, Y.-T. S. and S. Malik (1995, November). Performance analysis of embedded software using implicit path enumeration. *SIGPLAN Notices 30*, 88–98.

Lisper, B., A. Ermedahl, D. Schreiner, J. Knoop, and P. Gliwa (2010, October). Practical experiences of applying source-level WCET flow analysis on industrial code. In T. Margaria and B. Steffen (Eds.), *Proc. 4th International Symposium on Leveraging Applications of Formal Methods (ISOLA'10), Part II*, Volume 6416 of *Lecture Notes in Computer Science*, Heraclion, Crete, pp. 449–463. Springer-Verlag.

Michiel, M. D., A. Bonenfant, H. Cassé, and P. Sainrat (2008). Static loop bound analysis of c programs based on flow analysis and abstract interpretation. In *Proc. of the 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'08)*, Kaohsiung, Taiwan, pp. 161–166. IEEE.

NASA Engineering and Safety Center (2011, December). Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation. Technical report, Technical Assessment Report.

Nemer, F., H. Cassé, P. Sainrat, J.-P. Bahsoun, and M. D. Michiel (2006). Papabench: a free real-time benchmark. In F. Mueller (Ed.), *6th Intl. Workshop on Worst-Case Execution Time (WCET) Analysis*, Dagstuhl, Germany. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.

Pitter, C. and M. Schoeberl (2010). A real-time Java chip-multiprocessor. *ACM Trans. Embed. Comput. Syst. 10*(1), 9:1–34.

Prantl, A., J. Knoop, M. Schordan, and M. Triska (2008, December 12,). Constraint solving for high-level WCET analysis. In *Proceedings of the 18th Workshop on Logic-based Methods in Programming Environments (WLPE 2008)*, Udine, Italy, pp. 77–89. Computing Research Repository.

Prantl, A., M. Schordan, and J. Knoop (2008, July 1,). TuBound - A Conceptually New Tool for Worst-Case Execution Time Analysis. In *Post-Workshop Proceedings of the 8th International Workshop on Worst-Case Execution Time Analysis (WCET 2008)*, Volume 237, Prague, Czech Republic, pp. 141–148. Austrian Computer Society. Also: Schloß Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2008, ISBN 978-3-939897-10-1, 8 pages.

Ratsiambahotra, T., H. Cassé, and P. Sainrat (2009). A versatile generator of instruction set simulators and disassemblers. In *Proceedings of the 12th international conference on Symposium on Performance Evaluation of Computer & Telecommunication Systems*, SPECTS'09, Piscataway, NJ, USA, pp. 65–72. IEEE Press.

Schoeberl, M. (2008). A Java processor architecture for embedded real-time systems. *Journal of Systems Architecture 54/1–2*, 265–286.

Schoeberl, M., W. Puffitsch, R. U. Pedersen, and B. Huber (2010). Worst-case execution time analysis for a Java processor. *Software: Practice and Experience 40/6*, 507–542.

Souyris, J., E. L. Pavec, G. Himbert, V. Jégu, G. Borios, and R. Heckmann (2005). Computing the Worst Case Execution Time of an Avionics Program by Abstract Interpretation. In *Proceedings of the 5th International Workshop on Worst-Case Execution Time (WCET '05)*, Mallorca, Spain, pp. 21–24. OASIcs — OpenAccess Series in Informatics.

Tan, L. (2009, February). The worst-case execution time tool challenge 2006. *Int. J. Softw. Tools Technol. Transf. 11*, 133–152.

Wenzel, I., R. Kirner, B. Rieder, and P. P. Puschner (2008). Measurement-based timing analysis. In *Proc. 3rd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'08)*, Porto Sani, Greece, pp. 430–444. Springer.

Wilhelm, R., J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, and P. Stenström (2008). The worst-case execution-time problem—overview of methods and survey of tools. *ACM Transactions on Embedded Computing Systems (TECS) 7*(3), 36:1–36:53.

Zolda, M., S. Bünte, and R. Kirner (2011, August). Context-sensitive measurement-based worst-case execution time estimation. In *17th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'11)*, Toyama, Japan. IEEE. accepted.

Appendix

A The Target Processors

After polling the potential participants, we decided to suggest two common target processors for WCC'11, a "simple" processor and a "complex" processor. However, participants were welcome to use other processors as well.

A.1 The "Simple" Processor: ARM7

As "simple" processor, the same processor was selected as in WCC'08, the ARM7, as e. g. on the LPC2138 board from NXP Semiconductor. Its MAM (Memory Acceleration Module) was de-activated. The following is a brief description of the ARM7, based on the WCC'08 report.

The ARM7 (ARM 1995) is a simple, deterministic processor without caches and complex pipelines. It is a 32-bit pipelined RISC architecture with a single (von Neumann) address space. All basic ARM7 instructions are 32 bits long. Some ARM7 devices support the alternative THUMB instruction set, with 16-bit instructions, but this was not used in WCC'11. The ARM7 processor has 16 general registers of 32 bits. Register 15 is the Program Counter. Thus, when this register is used as a source operand it has a static value, and if it is a destination operand the instruction acts as a branch. Register 14 is designated as the "link register" to hold the return address when a subprogram call occurs. There are no specific call/return instructions; any instruction sequence that has the desired effect can be used. This makes it harder for static analysis to detect call points and return points in ARM7 machine code. The timing of ARM7 instructions is basically deterministic. Each instruction is documented as taking a certain number of "incremental" execution cycles of three kinds: "sequential" and "non-sequential" memory-access cycles and "internal" processor cycles. The actual duration of a memory-access cycle can depend on the memory subsystem. The term "incremental" refers to the pipelining of instructions, but the pipeline is a simple linear one, and the total execution-time of an instruction sequence is generally the sum of the incremental times of the instructions.

The LPC2138 chip The NXP LPC2138 implements the ARM7 architecture as a microcontroller with 512 KiB of on-chip flash memory starting at address zero and usually storing code, and 32 KiB of static on-chip random-access memory (SRAM) starting at address 0x4000 0000 and usually storing variable data. There is no off-chip memory interface, only peripheral I/O

(including, however, I2C, SPI, and SSP serial interfaces that can drive memory units).

The on-chip SRAM has a single-cycle (no-wait) access time at any clock frequency. The on-chip flash allows single-cycle access only up to 20 MHz clock frequency. At higher clock frequencies, up to the LPC2138 maximum of 60 MHz, the flash needs wait cycles. This can delay instruction fetching and other flash-data access. The LPC2138 contains the aforementioned device called the Memory Acceleration Module (MAM) that reduces this delay by a combination of caching and prefetching; however, as already mentioned, we suggested to de-activate the MAM.

The on-chip peripherals in the LPC2138 connect to a VLSI Peripheral Bus (VPB) which connects to the Advanced High-performance Bus (AHB) through an AHB-VPB bridge. This bus hierarchy causes some delay when the ARM7 core accesses a peripheral register through the AHB. If the VPB is configured to run at a lower clock frequency than the ARM7 core this delay is variable because it depends on the phase of the VPB clock when the access occurs.

The programming tools The IF-DEV-LPC kit from iSYSTEM came with an integrated development environment called WinIDEA and a GNU cross-compiler and linker. The distributed benchmark binaries for WCC'11 were created with Build 118 of these tools using gcc-4.2.2[14]. The IF-DEV-LPC kit has an USB connection to the controlling PC and internally uses JTAG to access the LPC2138. WinIDEA supports debugging with breakpoints, memory inspections, and so on.

A.2 The "Complex" Processor: MPC5553/5554

The Freescale MPC5553/MPC5554 micro-controllers implement the PowerPC Book E instruction set. The Book E instruction set adapts the normal PowerPC ISA to the special needs of embedded systems. The normal floating point instructions are replaced by digital signal processing instructions.

Both micro-controllers have a two-level memory hierarchy. They use a unified cache (8 KB on the MPC5553, 32 KB on the MPC5554) to accelerate the accesses to the internal SRAM and Flash memory. Additionally, they support the use of external memory. The memory management unit has a 32-entry translation look-aside buffer. The load/store subsystem is fully pipelined and an 8-entry store buffer is used to accelerate the instruction throughput.

The unified cache is 2-way set associative on the MPC5553 and 8-way set associative on the MPC5554. The cache can be locked on a per way basis. Moreover, a way can be declared as instruction or data cache only.

[14] `http://www.isystem.si/SWUpdates/Setup_IFDEV_9_7_118/iFDEVSetup.exe`

As another acceleration mechanism, the micro-controllers support branch prediction. The processors run at a clock speed of up to 132 MHz.

Various peripherals can be attached to the micro-controllers, for example by using the FlexCAN bus. The MPC55xx micro-controllers support debugging through the IEEE-ISTO 5001-2003 NEXUS interface and the IEEE 1149.1 JTAG controller.

A.3 The TriCore 1796

The TriCore 1796 and the TriBoard TC1796 were the chosen target of the FORTAS tool (see Sec. 2.4). The TC1796 is based on the 32-bit TriCore 1.3 load/store architecture. We focus on the features that we consider particularly relevant for execution timing and measurement. For details, please refer to the processor manual (Infineon 2007).

The TC1796 uses a Harvard architecture with separate buses to program and data memory, i.e., instruction fetching can be performed in parallel with data accesses. The 4GB address space is partitioned into 16 equally-sized segments. For the challenge, program code was stored in segment 8, which provides cached memory accesses via the *External Bus Unit* (EBU). The instruction cache is two-way set-associative with LRU replacement strategy. It has a line size of 256 bits. The cache can be globally invalidated and be globally bypassed. Unaligned accesses crossing caches line is supported with a penalty of 1 CPU cycle.

There is no data cache, but all data written by ST (store) or LDMST (load-modify-store) instructions is buffered. The buffer content is written to memory when the CPU and the Data Local Memory Bus are both idle.

Execution timing is also affected by the superscalar design. The TC1796 has a top-level pipeline consisting of an *Instruction Fetch Unit*, an *Execution Unit* and a *General Purpose Register File*. Within the execution unit the pipeline splits into three parallel sub-pipelines: an *Integer Pipeline*, which mainly handles data arithmetics and conditional jumps, a *Load Store Pipeline*, which is mainly responsible for memory accesses, unconditional jumps, calls and context switching, and a *Loop Pipeline*, which mainly handles special loop instructions providing zero-overhead loops. Consequently, up to three instructions can be issued and executed in parallel. Also, a floating point unit is attached to the CPU as a coprocessor. Furthermore, there is a static branch predictor that implements the following rules (Infineon 2003): Backward and short forward branches (16-bit branches with positive displacement) are predicted taken. Non-short forward branches are predicted not taken. The overhead of the different cases is summarized in Table 7.

The TC1796 offers *On-Chip Debug Support* (OCDS) *Level 1* and *Level 2* for debugging and execution time measurement. OCDS Level 1 includes a JTAG module, which can be used to download programs to the target

Prediction	Outcome	Penalty (cycles)
not taken	not taken	1
not taken	taken	3
taken	not taken	3
taken	taken	2

Table 7: Branch penalties.

and to inject input data. Tracing is enabled via OCDS Level 2, a vendor-specific variant of the *Nexus IEEE-ISTO 5001-2003* standard interface[15]. For the challenge, this interface was used to sample time-stamped program flow information at each CPU cycle without exerting a probing effect. Code instrumentation is not necessary.

Target Platform: TriBoard TC1796 We focus on those features particularly relevant for execution timing and measurement. Details can be found in the board manual (Infineon 2005b).

The TriBoard is equipped with 4MB of Burst Flash memory and 1 MB of asynchronous SRAM, which are both connected to the processing core via the External Bus Unit of the processor, and these are the only devices that are connected to the EBU. For the challenge, both program data and program instructions were placed into the asynchronous SRAM area.

The *Clock Generation Unit*, which is controlled by an external crystal oscillator, produces a clock signal f_{OSC} at 20MHz. The CPU clock runs at 150MHz, and the system clock at 75MHz.

A.4 The C167

The Infineon C167 (more precisely, the C167CR) 16-Bit CMOS Single-Chip Microcontroller has been used in the Challenge by TuBound, via the tool Calc_wcet_167 (see Sec. 2.9). It is a single-issue, in-order architecture with a jump cache. The C16x family of microcontrollers targets real-time embedded control applications and is optimized for high instruction throughput and low response time to external interrupts. It combines features of both RISC and CISC processors. Separate buses connect the program memory, internal RAM, (external) peripherals and on-chip resources. The CPU is clocked at 25/33 MHz allowing a 80/60 ns minimum instruction cycle time. Details can be found in the manual (Infineon 2005a).

The core of the CPU consists of a for 4-stage instruction pipeline, a 16-bit ALU, dedicated SFRs, separate multiply, divide, bit-mask generator

[15] `http://www.nexus5001.org/`

and barrel shifter units. Because of optimized hardware, most instructions can be executed in one machine cycle. Instructions requiring more than one cycle have been optimized. Branching, for example, requires only one additional cycle when a branch is taken. The pipeline is extended by a 'Jump Cache' that optimizes conditional jumps performed repeatedly in loops: most branches taken in loops require no additional cycles.

The memory of the C167 is a Von Neumann architecture, code memory, data memory, registers and IO ports are organized in the same 16MB linear address space. Memory can be accessed byte-wise or word-wise. Particular portions can be addressed bit-wise, which is supported by special instructions for bit-processing. A 2 KByte 16-bit wider internal RAM provides fast access to registers, user data and system stack.

A.5 The JOP Architecture

JOP is a Java processor especially optimized for embedded real-time systems (Schoeberl 2008). The primary design target of JOP is time-predictable execution of Java bytecodes, the instruction set of the Java virtual machine (JVM). JOP is designed to enable WCET analysis at the bytecode level. Several Java WCET tools target JOP; WCA (Schoeberl, Puffitsch, Pedersen, and Huber 2010), the WCET analysis tool that is part of the JOP distribution, was used in the WCET Challenge 2011 (see Sec. 2.10). JOP and WCA are available in open-source under the GNU GPL license.[16]

The JOP pipeline is as simple as the ARM7 pipeline. The main difference is that a translation of bytecodes to a sequence of microcode instructions is performed in hardware. Microcode instructions execute, as in standard RISC pipelines, in a single cycle. Bytecode instructions can execute in several cycles. The timing model for bytecode instructions is automatically derived from the microcode assembler code by WCA.

Bytecode instructions usually execute in constant time. Only for instructions that access main memory the access time has to be modeled. In WCA modeling of a simple SRAM memory is included and also a model of a chip-multiprocessor version of JOP with TDMA based memory arbitration (Pitter and Schoeberl 2010).

JOP contains three caches: a stack cache for stack allocated local variables, a method cache for instructions, and an object cache for heap allocated objects. The stack cache has to be large enough to hold the whole stack of a thread. Spill and fill of the stack cache happens only on thread switch. Therefore, a guaranteed hit in the stack cache can be assumed by WCA. The method cache stores whole methods and is loaded on a miss on a method invocation or on a return. WCA includes a static, scope-based persistence analysis of the method cache. The analysis of the object cache (Huber,

[16] see `http://www.jopwiki.com/Download`

Puffitsch, and Schoeberl 2011) is not yet completely integrated into WCA and we assume misses on all object field accesses for the WCET Challenge.

With the method cache JOP is slightly more complex than the ARM7 target. The reference configuration of JOP uses a 4 KB method cache and a 1 KB stack cache. The main memory is 32-bit, 1 MB of SRAM that has a read access time of 2 clock cycles and a write access time of 3 clock cycles.