

Verifying Digital Systems with MATLAB

Lennon Chaves and
Iury Bessa
Federal University of
Amazonas
lennonchaves@ufam.edu.br
iurybessa@ufam.edu.br

Lucas Cordeiro and
Daniel Kroening
University of Oxford
lucas.cordeiro@cs.ox.ac.uk
kroening@cs.ox.ac.uk

Eddie Filho
Samsung Electronics
eddie.1@samsung.com

ABSTRACT

A MATLAB toolbox is presented, with the goal of checking occurrences of design errors typically found in fixed-point digital systems, considering finite word-length effects. In particular, the present toolbox works as a front-end to a recently introduced verification tool, known as Digital-System Verifier, and checks overflow, limit cycle, quantization, stability, and minimum phase errors, in digital systems represented by transfer-function and state-space equations. It provides a command-line version, with simplified access to specific functions, and a graphical-user interface, which was developed as a MATLAB application. The resulting toolbox is important for the verification community, since it shows the applicability of verification to real-world systems.

Keywords

Embedded Digital Systems; MATLAB Toolbox; Software Model Checking; Formal Verification.

1. INTRODUCTION

Currently, digital systems (*e.g.*, filters and controllers) are used in a wide variety of applications, due to some advantages over their analog counterparts, such as reliability, flexibility, and cost. Nonetheless, there are disadvantages regarding their use: since they are normally implemented in microprocessors, errors might be introduced, due to quantization and related round-off effects [1].

Hardware choice, structure representations (*e.g.*, direct forms), and implementation features (*e.g.*, number of integer and fractional bits, in fixed-point arithmetic) can heavily influence a given digital-system's precision and performance [2]. Additionally, such implementations are particularly susceptible to finite word-length (FWL) effects (*e.g.*, overflows, limit cycles, and poles and zeros sensitivity), which have the potential to reduce the associated reliability and efficiency. Previous studies have already shown that FWL effects might lead to excessive power loss and lifespan reduction, in power converters [3] and oscillators [4]; they might

also affect the stability and performance of feedback control systems [5]. Thus, it is important to develop techniques that provide proof of correctness and safety, regarding digital-system implementations affected by FWL effects.

In order to detect the mentioned errors in digital systems, a model-checking procedure based on Boolean Satisfiability (SAT) and Satisfiability Modulo Theories (SMT) has been proposed, named as Digital-System Verifier (DSVerifier) [6]. DSVerifier checks specific properties related to overflow, limit cycle, stability, and minimum-phase, in digital-system implementations [2], and also supports the verification of robust stability, considering parametric uncertainties for closed-loop systems represented by transfer functions [7]. Recently, DSVerifier was extended to support state-space systems, considering single-input single-output (SISO) and multiple-input multiple-output (MIMO) systems [8], in order to verify violations in stability, controllability, observability, and quantization-error properties. Although those contributions present important advances regarding formal verification of digital systems, they do not offer any compatibility with tools usually employed in the design of digital filters and controllers (*e.g.*, MATLAB [9]).

Currently, there are several toolboxes in MATLAB with functions to facilitate the design of digital systems [9]. For instance, the fixed-point designer toolbox provides data-types and tools for developing fixed-point digital systems. There are also other modules with different objectives, such as optimization, control systems, and digital signal processing. In particular, users could employ formal verification methods to identify errors and generate test vectors for reproducing errors. In that sense, Simulink Design Verifier [9] employs formal methods to identify hidden design errors, without extensive simulation runs; it detects blocks that result in integer overflow, dead logic, array access, division by zero, and requirement violations. Additionally, it is possible to use tools for detecting and proving errors in source code written in C/C++, through Polyspace Bug Finder [9]. Nonetheless, both tools are unable to automatically detect specific errors related to digital system design (*e.g.*, limit cycle, stability, and minimum-phase), unless an engineer provides additional assertions to be checked [12]. Finally, the mentioned tools do not consider FWL effects during verification, and also, there is no MATLAB toolbox for verifying digital systems using symbolic model checking based on SAT and SMT solvers.

The present paper addresses this problem and presents a MATLAB toolbox for DSVerifier,¹ known as DSVerifier Toolbox, which applies SAT- and SMT-based model checking to digital systems [6], in the MATLAB's environment.

¹Available at <http://www.dsverifier.org>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

The main advantage regarding the use of a MATLAB toolbox lies on designing digital systems in MATLAB and then promptly verifying their desired properties: overflow, limit-cycle, stability, minimum-phase, controllability, observability, and quantization error. Additionally, when using the DSVerifier Toolbox, an engineer is able to design a digital system with MATLAB, through transfer-function or state-space representations and considering low-level systems parameters (implementation characteristics and numeric format), define realization forms (*e.g.*, delta and direct forms), and evaluate different overflow modes (wrap-around or saturate mode). Finally, if a verification procedure fails, the DSVerifier Toolbox returns a counterexample in a “.MAT” file, which explores the violation, considering inputs, initial states, and outputs, in order to reproduce a counterexample.

2. DSVERIFIER-AIDED VERIFICATION METHODOLOGY

The proposed verification methodology is based on DSVerifier and can be split into four steps. In step 1, a digital system is designed (in open- or closed-loop), with any design technique or tool. Later, implementation features are defined in step 2, *i.e.*, FWL format (number of bits in the integer and fractional parts), dynamic range, and realization form (direct or delta). DSVerifier formulates a FWL function $FWL[\cdot] : \mathcal{P}^n \rightarrow \mathcal{P}^n$, where \mathcal{P}^n is a space of polynomials of n -th order, in order to reproduce the effects of the chosen FWL format over the coefficients of a digital system. $FWL[A(z)]$ is the polynomial $A(z)$ with FWL effects that is used to compute round-off effects, in digital systems. Those definitions are then passed to DSVerifier, along with hardware specifications and other verification parameters (*e.g.*, verification time) and properties to be checked.

In particular, with respect to open-loop systems in transfer-function representation, DSVerifier supports verification of overflow, stability, minimum-phase, limit cycle, and quantization error properties, while it provides verification for stability, controllability, observability, and quantization properties, in state-space representation. Regarding closed-loop systems represented by a controller and a plant in transfer function form, DSVerifier is able to verify stability, quantization error, and limit-cycle, while it checks stability, controllability, observability, and quantization error, when state-space equations are employed.

Once the configuration has been set up in step 3, the verification process is then started in step 4, with the chosen model-checking tool (CBMC [10] or ESBMC [11] can be used as back-end). DSVerifier then checks the desired properties and returns “successful”, if there is no property violation in the proposed implementation, or “failed” together with a counterexample, which contains inputs and states that lead the system under evaluation to a given property violation. The implementation features and design should then be improved, based on the available counterexample, *i.e.*, realization, representation, and FWL format can then be re-chosen, in order to avoid errors. Finally, such a process is repeated until a digital controller implementation does not present any failure.

DSVerifier Toolbox uses bounded model checking (BMC) as verification engine. The basic idea of the BMC technique is to check the negation of a given property, at a given depth. Given a transition system M , a property ϕ , and a bound k , the employed verification engine unrolls the transition system k times and translates it into a verification

condition ψ , in such a way that ψ is satisfiable if and only if ϕ has a counterexample of depth less than or equal to k . Thus, overflow, limit cycle, and quantization errors, in transfer-function representation, and quantization error verification, when employing a state-space representation must be unrolled k times, in order to find violations (verification is incomplete, but sound up to k). In contrast, properties such as stability and minimum-phase, in transfer-function representation, and controllability, stability, and observability, in state-space representation, do not need a definition of k (verification is complete and sound).

3. VERIFYING DIGITAL SYSTEMS WITH DSVERIFIER TOOLBOX

3.1 The Employed Verification Methodology

Fig. 1 shows the proposed DSVerifier toolbox’s verification methodology, which can be split into two main stages: manual (user) and automated (toolbox) procedures. In the former, the user manually performs steps 1 to 3, which are the same tasks performed by DSVerifier (design of a digital-system, definition of numerical representation, realization form, and verification configuration). Note that all those specifications are provided as parameters (and translated to a struct format in the automated procedures performed by the toolbox), as can be seen in Fig. 1.

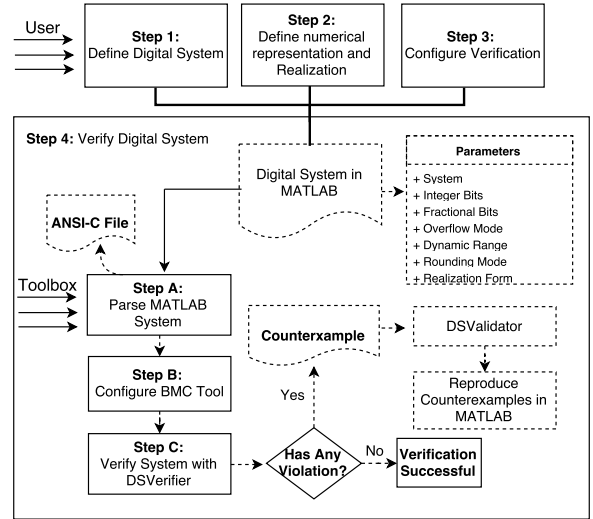


Figure 1: DSVerifier Toolbox’s Verification Methodology.

The toolbox’s automated engine (steps A to C) receives a digital system’s specification (as parameters) and verifies the desired property ϕ . In step A, intermediate ANSI-C code for the desired implementation is created, based on parameters that are then translated into a struct format (in MATLAB) and parsed, while the respective BMC tool is set and all requirements are configured in step B. Finally, in step C, the resulting ANSI-C code is passed to a highly-efficient BMC tool (*e.g.*, CBMC or ESBMC) and then converted into SAT or SMT formulae, which are checked by the respective solver. If any violation is found, then DSVerifier reports a counterexample, which contains system inputs that lead to a failure; otherwise, it returns a successful verification. In particular, in case of a failure, the proposed toolbox receives a

counterexample and generates a corresponding “.MAT” file. It is worth noticing that the same counterexample could be reproduced and validated with the DSValidator [12] tool.

3.2 DSVerifier Toolbox Features

1. **Digital-system representation:** DSVerifier Toolbox handles digital systems represented by transfer-function and state-space representations.
2. **Realization:** DSVerifier Toolbox performs the verification of direct forms, such as direct-form I (DFI), direct-form II (DFII), and transposed direct-form II (TDFII), and also delta forms, such as delta direct-form I (DDFI), delta direct-form II (DDFII), and delta transposed direct-form II (TDDFII).
3. **Properties:** DSVerifier Toolbox verifies, for transfer-function representation, stability, overflow, minimum phase, limit-cycle, and quantization error, while in state-space representation, it verifies stability, quantization error, observability, and controllability properties.
4. **Closed-loop systems:** DSVerifier Toolbox verifies stability, limit-cycle, and quantization error in transfer-function representation, while for state-space systems, all properties mentioned for open-loop systems are checked, via state feedback matrix.
5. **BMC tools:** DSVerifier Toolbox handles the verification for digital-systems using CBMC [10] or ES-BMC [11] as back-end, in order to perform BMC.

3.3 DSVerifier Toolbox Usage

In order to explain the DSVerifier Toolbox’s workflow, the following second-order controller for a A/C motor plant is used, which can be found in a set of benchmarks (*e.g.*, unmanned aerial vehicle) available online:²

$$H(z) = \frac{z^3 - 2.819z^2 + 2.6370z - 0.8187}{z^3 - 1.97z^2 + 1.033z - 0.06068}. \quad (1)$$

3.3.1 Command Line Version

Currently, users must provide a digital system described as a MATLAB system, *i.e.*, using a `tf` (for transfer-function) or an `ss` (for state-space) command, in order to design systems. In this command-line version, DSVerifier Toolbox is invoked to check the desired property ϕ and digital system representation (*i.e.*, transfer-function, closed-loop, or state-space). Table 1 shows the DSVerifier Toolbox’s commands that perform the proposed verification and the required parameters for each property. In particular, a k bound is required only in some properties, as mentioned in section 2. In Table 1, *system* represents the digital system in transfer-function or state-space format, *intbits* is the integer part, *fracbits* is the fractional part, *max* and *min* are the maximum and minimum dynamic range, respectively, *bound* is the k bound to be employed during verification, *cmode* is the connection mode, for closed-loop systems in transfer-function (series or feedback), and *error* is the maximum possible value in the quantization error check.

Additionally, optional parameters can be included, such as overflow mode, rounding mode, BMC tool, solver, quantization error mode, delta coefficient (for delta realization),

²<http://www.dsverifier.org/benchmarks>

and other attributes that DSVerifier supports.³ All available functions w.r.t. the DSVerifier Toolbox have been exhaustively tested and experimental results are available online.⁴

3.3.2 Illustrative Example

In order to illustrate the DSVerifier Toolbox’s usage, Fig. 2 shows the stability verification for the digital system specified in Eq. 1, using a fixed-point format $\langle 2, 13 \rangle$ and a dynamic range $[1, -1]$.

```
>> num = [1.0000 -2.8190 2.6370 -0.8187];
>> den = [1.0000 -1.9700 1.0330 -0.0607];
>> system = tf(num,den,0.001);
>>
>> verifyStability(system,2,13,1,-1);
>> VERIFICATION SUCCESSFUL
```

Figure 2: Verifying Stability for a digital-system designed in MATLAB, with a fixed-point format $\langle 2, 13 \rangle$.

If the fixed-point format is changed to $\langle 12, 3 \rangle$, for the same system described in Eq. 1, the verification indicates a failure, *i.e.*, the digital system is unstable, as can be seen in Fig. 3, which indicates that the DSVerifier Toolbox is able to correctly verify digital systems with different implementations.

```
>> verifyStability(system,12,3,1,-1);
>> VERIFICATION FAILED
```

Figure 3: Verifying Stability for a digital-system designed in MATLAB, with a fixed-point format $\langle 12, 3 \rangle$.

After verifying that the adopted digital system is unstable (*i.e.*, verification fails) with the fixed-point format $\langle 12, 3 \rangle$, the respective verification result can be confirmed by reproducing the counterexample generated by the DSVerifier Toolbox. As mentioned during the explanation of the proposed methodology, we can have a polynomial $A(z)$ with FWL effects, through the application of $\mathcal{FWL}[A(z)]$. In particular, we compute the roots of $\mathcal{FWL}[A(z)]$, in order to check stability. If any root has modulus equal or greater than one, then the system is unstable; otherwise, it is stable. When applying $\mathcal{FWL}[H(z)]$, with the first case (*i.e.*, $\langle 2, 13 \rangle$), and computing the roots of the denominator of $\mathcal{FWL}[H(z)]$, where $H(z)$ is introduced in Eq. 1 to represent a digital-system, we obtain the following set of poles: $I = \{0.9629, 0.9400, 0.0672\}$, from which one can conclude that all poles are inside the unit circle. This means that the mentioned system is stable, when the numeric representation $\langle 2, 13 \rangle$ is used; however, when applying $\mathcal{FWL}[H(z)]$ to the second case (*i.e.*, $\langle 12, 3 \rangle$) and then computing the denominator roots of $\mathcal{FWL}[H(z)]$, the following set of poles is obtained: $J = \{1.3090, 0.5000, 0.1910\}$, where set J has one root with modulus greater than one, which confirms that using $\langle 12, 3 \rangle$, as fixed-point format, the verified system becomes unstable.

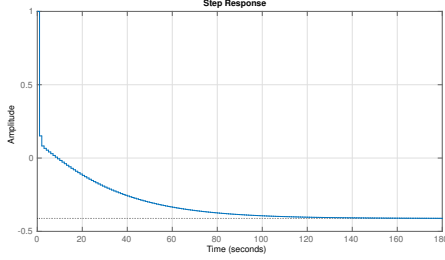
The stability for the digital systems described above could be indeed observed through the step response for both cases, as shown in Fig. 4. In subfigure 4(a), the step response shows that the digital system is stable, while in 4(b) it is unstable.

³All functions implemented in DSVerifier Toolbox are detailed in the Toolbox’s Documentation.

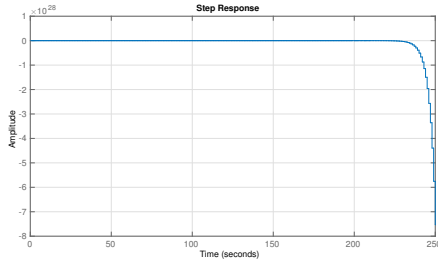
⁴<http://www.dsverifier.org/benchmarks>

Table 1: DSVerifier Toolbox’s commands and parameters used during verification procedures.

Verification Command	system	intbits	fracbits	max	min	bound	cmode	error
verifyStability	x	x	x	x	x			
verifyOverflow	x	x	x	x	x	x		
verifyError	x	x	x	x	x	x		x
verifyMinimumPhase	x	x	x	x	x			
verifyLimitCycle	x	x	x	x	x	x		
verifyClosedStability	x	x	x	x	x		x	
verifyClosedQuantizationError	x	x	x	x	x	x	x	x
verifyClosedLimitCycle	x	x	x	x	x	x	x	
verifyStateSpaceStability	x	x	x					
verifyStateSpaceControllability	x	x	x					
verifyStateSpaceObservability	x	x	x					
verifyStateSpaceQuantizationError	x	x	x			x		x



(a) Successful verification using the format (2, 13).



(b) Failed verification using the format (12, 3).

Figure 4: Step Response for Eq. (1).

3.3.3 GUI Application Version

A graphical user interface application was developed, in order to favor digital-system verification in MATLAB, besides improving usability and, consequently, attracting more digital-system engineers. Users can provide all required parameters for digital-system verification: digital-system specification, target implementation, and properties to be checked.

4. CONCLUSION

DSVerifier Toolbox is able to verify dynamic digital-systems (controllers or filters) designed in MATLAB, through transfer-function and state-space representations in open- or closed-loop format. Regarding transfer-function representations, users are able to verify stability, minimum-phase, limit-cycle, overflow, and quantization error properties, while in state-space format, stability, quantization error, observability, and controllability properties can be verified.

We have shown that a digital controller using different numerical representations can present distinct verification results. In particular, we demonstrated that a specific representation has the potential to cause instability and then

compromise the entire system’s operation. DSVerifier Toolbox can verify digital systems with different implementation aspects. Given the current knowledge in formal verification, there is no other MATLAB toolbox for verifying specific properties of digital systems, while taking into account implementation aspects.

As future work, DSVerifier Toolbox could perform verification for robust stability, by considering uncertainty in the plant and controller of closed-loop systems, and it could also be integrated into DSValidator [12].

5. REFERENCES

- [1] Diniz P., da Silva E., Netto S. (2010) “Digital Signal Processing: System Analysis and Design”. E-Libro, Cambridge University Press.
- [2] Bessa I. and *et al.* (2016) “Verification of fixed-point digital controllers using direct and delta forms realizations.” In *DAES.*, 20(2):95–126.
- [3] Peterchev A and *et al.* (2003) Quantization resolution and limit cycling in digitally controlled PWM converters. In *IEEE Trans. Power Electronics*, 18(1): pp.301–308.
- [4] Peretz M and *et al.* (2010) Digital Control of Resonant Converters: Resolution Effects on Limit Cycles. In *IEEE Trans. Power Electronics*, 25(6): pp. 1652–1661.
- [5] Keel L, Bhattacharyya S (1997) Robust, fragile, or optimal?. In *IEEE Trans. Automatic Control*, 42(8): pp. 1098–1105.
- [6] Ismail H. and *et al.* (2015) “DSVerifier: A Bounded Model Checking Tool for Digital Systems”. In *SPIN*, LNCS 9232, pp. 126–131.
- [7] Bessa I and *et al.* (2017) “Formal non-fragile stability verification of digital control systems with uncertainty”. In *IEEE Trans. Computers*, 66(3): pp. 545–552.
- [8] Monteiro, F. R. (2016) “Bounded Model Checking of State-Space Digital Systems”. In *FSE*, pp. 1151–1153.
- [9] Matlab Toolbox (2017). In <https://www.mathworks.com/products/>.
- [10] Kroening, D. and Tautschnig, M. (2014) “CBMC – C Bounded Model Checker,” In *TACAS*, LNCS 8413, pp. 389–391.
- [11] Cordeiro and *et al.* (2012) “SMT-Based Bounded Model Checking for Embedded ANSI-C Software,” In *TSE*, 38(4): pp. 957–974.
- [12] Chaves, L. and *et al.* (2016) “DSValidator: An Automated Reproducibility Tool for Digital Systems”, In Technical Report published as an arXiv Document.