DSSynth: An Automated Digital Controller Synthesis Tool for Physical Plants
ASE 2017

Alessandro Abate, Iury Bessa, Dario Cattaruzza, Lennon Chaves, Lucas Cordeiro, Cristina David, Pascal Kesseli, Daniel Kroening and Elizabeth Polgreen

Diffblue Ltd.,
University of Oxford,
Federal University of Amazonas

November 1st, 2017
Motivation
Motivation

Automatically synthesise digital controllers
Typical closed-loop control system

• Representation of the digital controller and plant
  ○ state-space: matrices $A$, $B$, $C$, and $D$
  ○ transfer-function: coefficients $b_0, b_1,\ldots,b_m$ and $a_0, a_1,\ldots,a_m$
Typical closed-loop control system

- **Representation of the digital controller and plant**
  - state-space: matrices $A$, $B$, $C$, and $D$
  - transfer-function: coefficients $b_0$, $b_1$, ..., $b_m$ and $a_0$, $a_1$, ..., $a_m$

- **Stability of closed-loop systems**
  - presents a bounded response for any bounded excitation
Typical closed-loop control system

- Representation of the digital controller and plant
  - state-space: matrices $A$, $B$, $C$, and $D$
  - transfer-function: coefficients $b_0, b_1, \ldots, b_m$ and $a_0, a_1, \ldots, a_m$

- Stability of closed-loop systems
  - presents a bounded response for any bounded excitation

- Safety of closed-loop systems
  - defines a requirement on the states of the model
Typical closed-loop control system

- Representation of the digital controller and plant
  - state-space: matrices $A$, $B$, $C$, and $D$
  - transfer-function: coefficients $b_0$, $b_1, \ldots, b_m$ and $a_0$, $a_1, \ldots, a_m$

- Stability of closed-loop systems
  - presents a bounded response for any bounded excitation

- Safety of closed-loop systems
  - defines a requirement on the states of the model

- Numerical errors (truncation and rounding)
Objectives

Generate sound digital controllers for stability and safety specifications with a very high degree of automation
Objectives

Generate sound digital controllers for stability and safety specifications with a very high degree of automation

- support for transfer-function and state-space representations in closed-loop form
Objectives

Generate sound digital controllers for stability and safety specifications with a very high degree of automation

- support for transfer-function and state-space representations in closed-loop form
- synthesize different numerical representations of the controller using CounterExample Guided Inductive Synthesis (CEGIS)
Objectives

Generate sound digital controllers for stability and safety specifications with a very high degree of automation

- support for transfer-function and state-space representations in closed-loop form
- synthesize different numerical representations of the controller using CounterExample Guided Inductive Synthesis (CEGIS)
- provide a MATLAB toolbox to synthesize digital controllers while taking into account finite word-length effects
The Proposed Synthesis Methodology

Phases of the controller synthesis:

- **Step 1:** Determine the representation: state-space or transfer-function
- **Step 2:** Define the physical plant coefficients and intervals
- **Step 3:** Define the numerical representation

DSSynth

- **Step A:** Parse MATLAB system to ANSI-C program
- **Step B:** Invoke DSSynth with the synthesis specification
- **Step C:** Synthesize the digital controller

Digital System in MATLAB

Digital Controller Synthesized
CEGIS for Control Systems

CEGIS with multi-staged verification:

1. Safety
2. Precision
3. Completeness

Program Search
BMC-based Verifier
Fixed-point Arithmetic Verifier
Completeness Verifier

Increase Unfolding Bound
Increase Precision

PASS
DONE
DSSynth Usage - Transfer Function

Physical plant for an unmanned aerial vehicle (UAV) plant:

\[ G(z) = \frac{B(z)}{A(z)} = \frac{-0.06875z^2}{z^2 - 1.696z + 0.7089}. \]  \hspace{1cm} (1)

Synthesizing the digital controller:

```matlab
>> num = [-0.06875 0 0];
>> den = [1.0000 -1.696 0.7089];
>> system = tf(num,den,0.002);
>> y = synthesize(system,8,8,1,-1);
>> SYNTHESIS SUCCESSFUL
>> y =
>> -0.9983z^2 + 0.09587 z + 0.1926
>> --------------------------------
>> z^2 + 0.5665 z + 0.75
```
Digital controller synthesized by DSSynth:

\[ C(z) = \frac{-0.9983^2 + 0.09587z + 0.1926}{z^2 + 0.5665z + 0.75}. \]

Computing the general equation (plant and controller):

```plaintext
>> num = [-0.99832 0.09587 0.1926];
>> den = [1 0.5665 0.75];
>> controller = tf(num,den,0.002);
>> num = [-0.06875 0 0];
>> den = [1.0000 -1.696 0.7089];
>> plant = tf(num,den,0.002);
>> sys = feedback(series(controller, plant),1)
>> sys =
>>  0.06863z^4 - 0.006591z^3 - 0.01324z^2
>> ---------------------------------------------------
>> 1.069 z^4 - 1.136 z^3 + 0.4849 z^2 - 0.8704 z + 0.5317
```
Step response for the UAV plant describing a stable system:
(a) Definition of the system representation and the physical plant

(b) Definition of implementation aspects and input ranges
(c) Digital controller synthesized by DSSynth

(d) Step response for the synthesized digital controller
Experimental Evaluation

Our evaluation consists of 18 Single-Input and Single-Output control system benchmarks extracted from the literature:
Experimental Evaluation

Our evaluation consists of 18 Single-Input and Single-Output control system benchmarks extracted from the literature:

**Experimental Objectives:**

- Evaluate the DSSynth performance to produce digital controllers
- Confirm the stability and safety outside of our model using MATLAB
Experimental Evaluation

Our evaluation consists of 18 Single-Input and Single-Output control system benchmarks extracted from the literature:

**Experimental Objectives:**

- Evaluate the DSSynth performance to produce digital controllers
- Confirm the stability and safety outside of our model using MATLAB

**Experimental Setup:**

- Signal input range: $\langle-1, 1\rangle$
- Implementation features: $\langle8, 8\rangle$
- Intel Core i7 – 2600 3.40 GHz processor with 24 GB of RAM
Experimental Evaluation

Experimental Results:

• The digital controller order ranges from 1 to 8
Experimental Evaluation

Experimental Results:

- The digital **controller order** ranges from 1 to 8
- The number of **state variables** ranges from 1 to 9
Experimental Evaluation

Experimental Results:

- The digital controller order ranges from 1 to 8
- The number of state variables ranges from 1 to 9
- The average synthesis time amounts to 35.5 s for state-space systems
Experimental Evaluation

Experimental Results:

- The digital controller order ranges from 1 to 8
- The number of state variables ranges from 1 to 9
- The average synthesis time amounts to 35.5 s for state-space systems
- The average synthesis time amounts to 123.6 s for transfer functions
Experimental Evaluation

Experimental Results:

- The digital **controller order** ranges from 1 to 8
- The number of **state variables** ranges from 1 to 9
- The average synthesis time amounts to 35.5 s for state-space systems
- The average synthesis time amounts to 123.6 s for transfer functions
- On average our engine spent 52% in the synthesis and 48% in the verification phase
Experimental Evaluation

Experimental Results:

- The digital **controller order** ranges from 1 to 8
- The number of **state variables** ranges from 1 to 9
- The average synthesis time amounts to 35.5 s for state-space systems
- The average synthesis time amounts to 123.6 s for transfer functions
- On average our engine spent 52% in the synthesis and 48% in the verification phase

**DSSynth Matlab toolbox:**
https://www.cprover.org/DSSynth/dssynth-toolbox-1.0.0.zip
https://github.com/ssvlab/dsverifier/tree/master/toolbox-dssynth