Verification of Control Laws Using Formal Methods

Kestutis Siaulys
Jan Maciejowski
University of Cambridge
Introduction

➢ The problem

- Validation and verification of advanced feedback control laws used in safety critical systems (e.g. flight control) where the cost of failure is high.

➢ The solution

- We propose a novel way of verifying properties of controls systems by using an automated theorem prover MetiTarski [1], which is capable of proving universally quantified inequalities over a continuous range of uncertain real parameters like

\[ \forall \omega, (20\log_{10}|L(j\omega)|)^2 P_m^2 + (\angle L(j\omega) + \pi)^2 G_m^2 - (G_m P_m)^2 > 0. \]

by bounding functions like log10(x) and arctan(x) with polynomials obtained from Taylor series and continued fraction expansions.

Advantages of formal methods

- **Proofs are executed over a continuous range of real variables, hence formal methods approaches do not face issues experienced by methods which use gridding.**

- **Ability to prove verification requirements involving real functions like** \( \sin(x) \), \( \cos(x) \), \( \exp(x) \), \( \log_{10}(x) \), \( \arctan(x) \).

- **It provides an actual mathematical proof of the statement in full precision arithmetic that can be checked manually by a human or automatically by an independent verification tool.**

- **No need for repeated visual inspection for clearance criteria expressed as exclusion regions in Nyquist and Nichols planes.**
Verification framework

Verification criterion of interest

Algebraic manipulation

Inequality A over real parameters expressed in formal syntax

MetiTarski

"Theorem"

System meets the specified criterion

"Gave Up"

Polynomial inequality (NOT A) over real parameters

"No"

Does inequality A contain real functions?

"Yes"

Verification test is inconclusive

"Theorem"

System does NOT meet the specified criterion
Application example

➢ A flight controller [2] where 55 control laws are computed based on 234 flight points, and each control law is applicable at multiple flight points.

Verification criterion: complementary sensitivity function

\[ |T(j\omega)| = \left| \frac{L(j\omega)}{1 + L(j\omega)} \right| \leq 1\text{dB} \]

for all flight points (FP) corresponding to control law #17.

Equivalent condition: M-circle \((M = 10^{0.05})\) exclusion region in the Nyquist plane with \(x_c = -4.86, r = 4.33\).

\[ \forall \omega, \ (\Re(L(j\omega)) - x_c)^2 + (\Im(L(j\omega)))^2 > r^2. \]

Proof results:
FP 79, 80, 81, 82: pass
FP 83: fail

Application example

Matches with results obtained graphically:

![Nyquist Diagram](image)

- FP 79 VCAS = 210 kts
- FP 80 VCAS = 240 kts
- FP 81 VCAS = 270 kts
- FP 82 VCAS = 300 kts
- FP 83 VCAS = 335 kts
Application example

➢ Matches with results obtained graphically:

![Nichols Chart](image)

- Open-Loop Phase (deg)
- Open-Loop Gain (dB)

-180  -135  -90  -45  0

-40  -30  -20  -10  0  10  20  30  40

-40 dB  -30 dB  -20 dB  -12 dB  -6 dB  -3 dB  -1 dB  0 dB  0.25 dB  0.5 dB  1 dB  3 dB  6 dB  12 dB  20 dB  40 dB
Application example

➢ Matches with results obtained graphically:

Magnitude plot of complementary sensitivity $T$

- Frequency (rad/s)
- Magnitude (dB)

-10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10

FP 79 VCAS = 210 kts
FP 80 VCAS = 240 kts
FP 81 VCAS = 270 kts
FP 82 VCAS = 300 kts
FP 83 VCAS = 335 kts
Conclusions and future work

➢ Conclusions:
  ▪ Verification framework for clearance of control laws via formal methods has been created.
  ▪ The framework has been used to clear several properties of flight control laws of interest.

➢ Future work:
  ▪ Clearing various verification criteria throughout the whole flight envelope, with gain-scheduled control laws.
  ▪ Comparison of formal methods verification framework with various classical analysis approaches, including structured singular value μ and sum of squares (SOS) techniques.