

# Symbolic Reasoning Applied to Control Laws

## Avenues of Research

Richard Boulton  
School of Computer Science  
University of St Andrews

18 April 2002

This document attempts to summarise the possible avenues of research identified so far in the QinetiQ-funded control engineering project in the School of Computer Science, University of St Andrews. It does not consider what resources would be required to conduct the research, e.g. theory support in the chosen theorem prover. It is not St Andrews' intention to investigate all of the identified topics during the current period of funding. One purpose of this document is to assist in the selection of one or two topics on which to focus.

### 1 Summary of Interesting Properties of Dynamic Systems

- Stability (in various forms).
  - Analyse using a step-function input.
  - Use the closed-loop transfer function.
- Frequency response: gain (amplitude) and phase shift.
  - Analyse using a sinusoidal input.
  - Both open-loop and closed-loop response are of interest.
- Handling properties:
  - rise time,
  - damping,
  - steady-state behaviour.

### 2 Bounds on Curves

In the analysis of frequency response, a number of graphical representations are used including Bode diagrams (two separate plots, one of gain against frequency, the other of phase against frequency), and Nichols charts (gain against phase as frequency varies). The shape and path of these graphs are used by engineers to determine the response of the system being modelled. Possible research topics include:

- Verifying that the Nichols plot remains outside polygonal exclusion regions such as those described by GARTEUR [1, pages 43–47].
  - Developing criteria for common cases of transfer function.
- What should be proved?
  - We could try to obtain symbolic expressions for the conditions on the transfer function that will keep the curve out of the exclusion regions, and prove this formally.
  - Or we could prove each case individually having instantiated the coefficients of the parameterised transfer function.
  - What about proving continuity and differentiability of the functions? These properties may be necessary to ensure a valid analysis of the path of the plot.
- We could do a similar analysis for bounds on Bode diagrams.
- We could do a similar analysis for discrete-time Bode and Nichols plots.
- Consider bounds on amplitude that ensure some limit (e.g. extent of rudder movement) is not exceeded. This analysis should allow any shape of input, not just step, ramp, and sinusoidal inputs.
- These ideas about placing bounds on plots might extend to properties that cannot be represented graphically.

### 3 Connections Between the Continuous and Discrete Models

- Investigate the relationship between continuous-time and discrete-time Bode and Nichols plots. This might arise as a consequence of trying to prove bounds on both continuous-time and discrete-time plots.
- Find out what modifications the engineers make to their continuous-time models so that they more closely match the corresponding discrete-time model. Is phase shifting to compensate for the zero-order hold one of the modifications (or *the* modification) that the engineers make? Is there any interesting relationship that we could prove something about?
- Investigate the relationship between stability conditions for the two time-domains. We have looked at this already, but there are lots of variations to investigate, e.g. we could compare the continuous-time model with the discrete-time model after the former has been modified as discussed above.

### 4 Composability

The transfer function of a full real-world system will typically be too large for formal analysis to be practical if the function is treated as a monolithic entity. We are therefore interested in finding properties that can be determined by composing properties of the individual components that make up the system. For example, it appears that the phase shift of a system

consisting of a controller and plant in sequence is the sum of the phase shift of the controller and the phase shift of the plant. Some possible research along these lines is as follows.

- Consideration of larger (open-loop) systems composed of several transfer functions. Gains should multiply, and phases add. E.g. a constraint on phase shift for a full system could be decomposed into constraints on the phase shift for the components.
- Build some kind of calculus around the above, or something akin to a Floyd-Hoare logic [3, 5]. There is a wide range of degrees of formalisation possible here, ranging from extracting verification conditions using something like ClawZ [2], through to “embedding” the calculus (or Floyd-Hoare logic) in the logic of a theorem prover [4] and proving that the properties of the calculus follow from a formalisation of the control theory (Laplace transforms, etc.).
- Extend the above to systems involving (closed) loops. Initial experiments suggest that general formulas for the gain and phase of a closed-loop system can be obtained in terms of the gain and phase of the corresponding open-loop system, but the independence between the gain and phase is lost. Hence, gain and phase would have to be treated together in any calculus. I.e. it would not be possible to have one calculus for gain, and another for phase.
- Determine bounds on curves by composing (probably adding) gain and phase values arising out of the factors of the numerator and denominator of the transfer function. It is not obvious that this is possible.
- Investigate how (if at all) composability works in the discrete-time domain, and repeat the above. This is arguably more industrially relevant than the continuous-time version.

## 5 Integration with Simulink

Ultimately, we want to offer formal analysis of the control system models to the control engineers and verification engineers. This might take the form of “batch processing” similar to the way ClawZ operates, using Simulink model files as the communication medium between tools. Alternatively, an interactive facility might be provided that adds new functions to MATLAB. These alternatives are described in more detail below.

- Use ClawZ with a new library to translate Simulink model files into Z. This could work well with the composability research outlined above. It could range from producing Z specifications for particular properties, to using ClawZ to translate the Simulink model into a calculus/logic/language embedded in a theorem prover.
- Alternatively, inter-process communication could be established between MATLAB, ProofPower, and Maple. This would allow new ways of operating. For example, for properties that can be proved automatically, Simulink might be extended with an on-the-fly (as opposed to batch/off-line) proof facility. The idea would be to put some formal verification in the hands of the control engineers, without them necessarily realising that formal proof was being used.<sup>1</sup>

---

<sup>1</sup>This was, in essence, the vision of the PROSPER project: <http://www.dcs.gla.ac.uk/prosper/>

## 6 Advanced Topics

Below is a summary of other avenues of research that we gleaned from discussions with control engineers but which we consider to be topics for consideration only after substantial research on simpler problems.

- Dealing with models of flexible aircraft?
- Dealing with non-linearity (variation with amplitude).
- Multi-input/multi-output systems with cross-coupling.
- Allowing mass and position of centre-of-gravity to vary within bounds. This might involve proving that a system remains stable (or has the desired handling properties) within certain (symbolic) bounds.
- Assertions about the response during transitions between flight modes, especially when mode switching is frequent.
- Investigate assertions about the effects of moving from sub-sonic to super-sonic flight, and vice versa.

## References

- [1] Action Group FM(AG08). Robust flight control design challenge problem formulation and manual: the high incidence research model (HIRM). Technical Report TP-088-4, version 3, Group for Aeronautical Research and Technology in Europe (GARTEUR), [garteursecretary@inta.es](mailto:garteursecretary@inta.es), April 1997.
- [2] R. Arthan, P. Caseley, C. O'Halloran, and A. Smith. ClawZ: Control laws in Z. In *Proceedings of the 3rd IEEE International Conference on Formal Engineering Methods (ICFEM 2000)*, York, UK, September 2000.
- [3] R. W. Floyd. Assigning meanings to programs. In *Proceedings of the American Mathematical Society Symposia in Applied Mathematics*, volume 19, pages 19–32, 1967.
- [4] M. J. C. Gordon. Mechanizing programming logics in higher order logic. In G. Birtwistle and P. A. Subrahmanyam, editors, *Current Trends in Hardware Verification and Automated Theorem Proving*, pages 387–439. Springer-Verlag, 1989. Also available as University of Cambridge Computer Laboratory Technical Report 145.
- [5] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 583, October 1969.