SPECIFICATION, DESIGN AND VERIFICATION OF DISTRIBUTED EMBEDDED SYSTEMS

AFOSR GRANT FA9550-06-1-0303

K. Mani Chandy John C. Doyle Richard M. Murray (PI)
California Institute of Technology

Eric Klavins
University of Washington

Pablo A. Parrilo
Massachusetts Institute of Technology

10 June 2011

Abstract We are investigating the specification, design and verification of distributed systems that combine communications, computation and control in dynamic, uncertain and adversarial environments. Our goal is to develop methods and tools for designing control policies, specifying the properties of the resulting distributed embedded system and the physical environment, and proving that the specifications are met. Accomplishments in this project over the last year include the development of new methods for synthesizing control protocols from linear temporal logic specifications, development of a framework to reason about information flow in terms of partially ordered sets (posets) and the development of a compositional framework for programming stochastically interacting robots.

Accomplishments

The design of reliable embedded control systems inherits the difficulties involved in designing both control systems and distributed (concurrent) computing systems. Design bugs in these systems may arise from the unforeseen interactions among the computing, communication and control subsystems. Motivated by the difficulties of finding this type of design bug, we have developed mathematical frameworks, based on formal methods, to facilitate the design and analysis of such embedded systems.

Distributed Computing and Decision-Making The problems of distributed computing and decision-making are central to the MURI. We seek to develop methods for both design and verification of cooperative control systems and other distributed protocols.

Applying Formal Methods to Distributed Systems Using Local-Global Relations [14] This thesis deals with the design and analysis of distributed systems in which homogeneous, autonomous agents collaborate to achieve a common goal. The class of problems studied includes consensus algorithms in which all agents eventually come to an agreement about a specific action. The thesis proposes a framework, called local-global, for analyzing these systems. The design challenge is to ensure that sequences of local interactions lead, or converge, to the same state as a global interaction. The local-global framework addresses this challenge by describing each local interaction as if were a global one, encompassing all agents within the system. This thesis outlines the concept in detail, using it to design algorithms, prove their correctness, and ultimately develop executable implementations that are reliable.

Decentralized Multi-Agent Optimization via Dual Decomposition [13] We study a distributed multi-agent optimization problem of minimizing the sum of convex objective functions. A new decentralized optimization algorithm is introduced, based on dual decomposition, together with the subgradient method for finding the optimal solution. The iterative algorithm is implemented on a multi-hop network and is designed to handle communication delays. The convergence of the algorithm is proved for communication networks with bounded delays. An explicit bound, which depends on the communication delays, on the convergence rate is given. A numerical comparison with a decentralized primal algorithm shows that the dual algorithm converges faster, with less communication.

Systematic Design and Formal Verification of Multi-Agent Systems [8] This thesis presents methodologies for verifying the correctness of multi-agent systems operating in hostile environments. We first consider message-passing multi-agent systems operating over an unreliable communication medium. We assume that messages in transit may be lost, delayed or received out-of-order. We present conditions on the system that reduce the design and verification of a message-passing system to the design and verification of the corresponding shared-state system operating in a friendly environment. Our conditions can be applied both to discrete and continuous agent trajectories. We apply our results to verify a general class of multi-agent system whose goal is solving a system of linear equations. We discuss this class in detail and show that mobile robot linear pattern-formation schemes are instances of this class.

Load balancing for multi-robot construction [7] In distributed multi-robot construction it is important to set the relative rates at which different construction sites receive raw building materials. Otherwise, subtasks finish at different times introducing unnecessary delays. We present a feedback algorithm to achieve robust load balancing in routing building materials for stochastic, distributed, multi-robot construction systems. We express global behavior in terms of local reactive behavior via *Guarded Command Programming with Rates* and prove correctness of the load-balancing controller for a wide range of conditions. We adapt a proof from earlier work on controlling Stochastic Chemical Kinetic systems and illustrate the algorithm on the Factory-Floor robotic testbed.

Stochastic Behavior and Games A key feature in understanding complex, distributed systems is the development of mechanisms for handling uncertainty. This uncertainty can be in the form of environmental disturbances and/or adversarial action. We are extending the formulations being developed for verification of hybrid systems to account for stochastic behavior, including game-theoretic approaches.

Tree-Structured Statistical Modeling via Convex Optimization [9] We develop a semidefinite-programming-based approach to the realization problem for a class of stochastic processes indexed by the vertices of a tree. We aim to construct a process indexed by a given tree such that the covariance among the leaf-variables realizes (or approximately realizes) a given covariance matrix. Unlike previous approaches to this problem, our method is global in nature and does not require prior specification of, or bounds on, the state dimensions at each vertex. Furthermore, we give conditions on a tree-structured process under which our approach correctly identifies the parameters and state dimensions of the underlying process given only the covariance among the leaf-variables. Finally we demonstrate, using a synthetic example, that given i.i.d. samples of the leaf-variables our method can identify the correct state dimensions of the underlying process.

A Compositional Framework for Programming Stochastically Interacting Robots [6] Large collections of simple, interacting robots can be difficult to program due to issues of concurrency and intermittent, probabilistic failures. Here, we present Guarded Command Programming with Rates, a formal framework for programming such multi-robot systems. Within this framework, we model robot behavior as a stochastic process and express concurrency and program composition using simple operations. In particular, we show how composition and other operations on programs can be used to specify increasingly complex behaviors of multi-robot systems and how stochasticity can be used to create programs that can tolerate failure of individual robots. Finally, we demonstrate our approach by encoding algorithms for routing parts in an abstract model of the Stochastic Factory Floor testbed (Galloway et al. 2010).

Setpoint Regulation for Stochastically Interacting Robots [5] We present an integral feedback controller that regulates the average copy number of a particular assembly in a system of stochastically interacting robots. The mathematical model for the stochastic system is a tunable reaction network, which makes this approach applicable to a large class of other systems, including ones that exhibit stochastic self assembly at various length scales. We prove that this controller works for a range of set-points, and how to compute this range. Finally, we demonstrate the approach on a physical testbed.

Verification and Design of Hybrid Systems We are also investigating design-oriented techniques for developing and verifying protocols and control laws for hybrid systems. These results are motivated by work on autonomous navigation of ground and space vehicles (the latter developed jointly with JPL).

Model checking with bounded context switching [4] We discuss the implementation of a bounded context switching algorithm in the Spin model checker. The algorithm allows us to find counter-examples that are often simpler to understand, and that may be more likely to occur in practice. We discuss extensions of the algorithm that allow us to use this new algorithm in combination with most other search modes supported in Spin, including partial order reduction and bitstate hashing. We show that, other than often assumed, the enforcement of a bounded context switching discipline does not decrease but increases the complexity of the model checking procedure. We discuss the performance of the algorithm on a range of applications.

TuLiP: A Software Toolbox for Receding Horizon Temporal Logic Planning [15] This paper describes TuLiP, a Python-based software toolbox for the synthesis of embedded control software that is provably correct with respect to an expressive subset of linear temporal logic (LTL) specifications. TuLiP combines routines for (1) finite state abstraction of control systems, (2) digital design synthesis from LTL specifications, and (3) receding horizon planning. The underlying digital design synthesis routine treats the environment as adversary; hence, the resulting controller is guaranteed to be correct for any admissible environment profile. TuLiP applies the receding horizon framework, allowing the synthesis problem to be broken into a set of smaller problems, and consequently alleviating the computational complexity of the synthesis procedure, while preserving the correctness guarantee.

Distributed Synthesis of Control Protocols for Smart Camera Networks We consider the problem of synthesizing control protocols for smart camera networks where the goal is to guarantee that certain linear temporal logic (LTL) specifications related to a given surveillance task are met. We first present a centralized control architecture for assigning pan-tilt-zoom (PTZ) cameras to targets so that the specification is met for any admissible behavior of the targets. Then, in order to alleviate the computational complexity associated with LTL synthesis and to enable implementation of local control protocols on individual PTZ cameras, we propose a distributed synthesis methodology. The main idea is to decompose the global specification into local specifications for each PTZ camera. A thorough design example is presented to illustrate the steps of the proposed procedure.

Fault-Tolerant Controller Design with Applications in Power Systems and Synthetic Biology [12] This paper deals with fault-tolerant controller design for linear time-invariant (LTI) systems with multiple actuators. Given some critical subsets of the actuators, it is assumed that every combination of actuators can fail as long as the set of the remaining actuators includes one of these subsets. Motivated by electric power systems and biological systems, the goal is to design a controller so that the closed-loop system satisfies two properties: (i) stability under all permissible sets of faults and (ii) better performance after clearing every subset of the existing faults in the system. It is shown that a state-feedback controller satisfying these properties exists if and only if a linear matrix inequality (LMI) problem is feasible. This LMI condition is then transformed into an optimal-control condition, which has a useful interpretation. The results are also generalized to output-feedback and decentralized control cases. The efficacy of this work is demonstrated by designing fault-tolerant speed governors for a power system. The results developed here can be extended to more general types of faults, where each fault can possibly affect all state-space matrices of the system.

Sum of Squares, Rank Sparsity and Lyapunov Analysis Finally, we continue to perform research that builds on our earlier work in sum-of-squares analysis for nonlinear and hybrid systems. This fundamental research area underlies many of the techniques described above.

An Optimal Controller Architecture for Poset-Causal Systems [11] We consider the class of decentralized systems known as poset-causal systems studied in [10]. While computational procedures for computing optimal decentralized controllers are now known [10], a detailed analysis of the architecture of the optimal controller is lacking. In this paper we propose a natural architecture for poset-causal controllers. In the process, we establish interesting connections between concepts from order theory such as Moëbius functions and control-theoretic concepts such as state estimation, innovation, and separability principles. Finally, we prove that the H2-optimal controller in fact possesses the proposed controller structure, thereby proving its optimality.

The Convex Geometry of Linear Inverse Problems [2] In applications throughout science and engineering one is often faced with the challenge of solving an ill-posed inverse problem, where the number of available measurements is smaller than the dimension of the model to be estimated. However in many practical situations of interest, models are constrained structurally so that they only have a few degrees of freedom relative to their ambient dimension. This paper provides a general framework to convert notions of simplicity into convex penalty functions, resulting in convex optimization solutions to linear, underdetermined inverse problems. The class of simple models considered are those formed as the sum of a few atoms from some (possibly infinite) elementary atomic set; examples include well-studied cases such as sparse vectors and low-rank matrices, as well as several others including sums of a few permutations matrices, low-rank tensors, orthogonal matrices, and atomic measures. The convex programming formulation is based on minimizing the norm induced by the convex hull of the atomic set; this norm is referred to as the atomic norm. The facial structure of the atomic norm ball carries a number of favorable properties that are useful for recovering simple models, and an analysis of the underlying convex geometry provides sharp estimates of the number of generic measurements required for exact and robust recovery of models from partial information. These estimates are based on computing the Gaussian widths of tangent cones to the atomic norm ball. When the atomic set has algebraic structure the resulting optimization problems can be solved or approximated via semidefinite programming. The quality of these approximations affects the number of measurements required for recovery. Thus this work extends the catalog of simple models that can be recovered from limited linear information via tractable convex programming.

Convex graph invariants [3] The structural properties of graphs are usually characterized in terms of invariants, which are functions of graphs that do not depend on the labeling of the nodes. In this paper we study convex graph invariants, which are graph invariants that are convex functions of the adjacency matrix of a graph. Some examples include functions of a graph such as the maximum degree, the MAXCUT value (and its semidefinite relaxation), and spectral invariants such as the sum of the k largest eigenvalues. Such functions can be used to construct convex sets that impose various structural constraints on graphs, and thus provide a unified framework for solving a number of interesting graph problems via convex optimization. We give a representation of all convex graph invariants in terms of certain elementary invariants, and describe methods to compute or approximate convex graph invariants tractably. We also compare convex and non-convex invariants, and discuss connections to robust optimization. Finally we use convex graph invariants to provide efficient convex programming solutions to graph problems such as the deconvolution of the composition of two graphs into the individual components, hypothesis testing between graph families, and the generation of graphs with certain desired structural properties.

Converse Results on Existence of Sum of Squares Lyapunov Functions [1] Despite the pervasiveness of sum of squares (sos) techniques in Lyapunov analysis of dynamical systems, the converse question of whether sos Lyapunov functions exist whenever polynomial Lyapunov functions exist has remained elusive. In this paper, we first show via an explicit counterexample that if the degree of the polynomial Lyapunov function is fixed, then sos programming can fail to find a valid Lyapunov function even though one exists. On the other hand, if the degree is allowed to increase, we prove that existence of a polynomial Lyapunov function for a homogeneous polynomial vector field implies existence of a polynomial Lyapunov function that is sos and that the negative of its derivative is also sos. The latter result is extended to develop a converse sos Lyapunov theorem for robust stability of switched linear systems.

Acknowledgment/Disclaimer

This work was sponsored (in part) by the Air Force Office of Scientific Research, USAF, under grant/contract number FA9550-06-1-0303. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Office of Scientific Research or the U.S. Government.

References

(Due to page limitations, this list contains only selected papers submitted or published during the past year. Preprints are available via the MURI website.)

[1] A. Ahmadi and P. A. Parrilo. Converse results on existence of sum of squares lyapunov functions amir. In *Proc. IEEE Control and Decision Conference*, 2011.

[2] V. Chandrasekaran, B. Recht, P.A. Parrilo, and A.S. Willsky. The convex geometry of linear inverse problems. Technical report, arXiv:1012.0621v1, 2011.

[3] V. Chandrasekaran, B. Recht, P.A. Parrilo, and A.S. Willsky. Convex graph invariants. Technical report, arXiv:1012.0623v1, 2011.

[4] G. J. Holzmann and M. Florian. Model checking with bounded context switching. *Formal Aspects of Computing*, 23(3):365–389, 2011.

[5] N. Napp, S. Burden, and E. Klavins. Setpoint regulation for stochastically interacting robots. *Autonomous Robotics*, 30(1):57–71, 2011.

[6] N. Napp and E. Klavins. A compositional framework for programming stochastically interacting robots. *International Journal of Robotics Research*, 30(6):713–729, 2011.

[7] N. Napp and E. Klavins. Load balancing for multi-robot construction. In *Proc. IEEE International Conference on Robotics and Automation*, 2011.

[8] C. Pilotto. *Systematic Design and Formal Verification of Multi-Agent Systems.* PhD thesis, California Institute of Technology, 2011.

[9] J. Saunderson, V. Chandrasekaran, P. A. Parrilo, and A. S. Willsky. Tree-structured statistical modeling via convex optimization. In *Proc. IEEE Control and Decision Conference*, 2011. Submitted.

[10] P. Shah and P. A. Parrilo. H2-optimal decentralized control over posets: A state-space solution for state-feedback. In *IEEE Transactions on Automatic Control*, 2011. Submitted.

[11] P. Shah and P. A. Parrilo. An optimal controller architecture for poset-causal systems. In *Proc. IEEE Control and Decision Conference*, 2011. Submitted.

[12] S. Sojoudi, J. Lavaei, and R. M Murray. Fault-tolerant controller design with applications in power systems and synthetic biology. In *Proc. American Control Conference*, 2011.

[13] H. Terelius, U. Topcu, and R. M. Murray. Decentralized multi-agent optimization via dual decomposition. In *Proc. IFAC World Congress*, 2011.

[14] J. White. *Applying Formal Methods to Distributed Systems Using Local-Global Relations.* PhD thesis, California Institute of Technology, 2011.

[15] T. Wongpiromsarn, U. Topcu, N. Ozay, H. Xu, and R. M. Murray. Tulip: A software toolbox for receding horizon temporal logic planning. In *Hybrid Systems: Computation and Control*, 2011.

Personnel Supported During Duration of Grant

Faculty: K. Mani Chandy (Caltech), John C. Doyle (Caltech), Eric Klavins (U. Washington), Richard M. Murray (Caltech), Pablo Parrilo, Michel Charpentier (visiting professor, Caltech)
Postdocs: Aaron Ames (Caltech; Assistant professor, Texas A&M), Sayan Mitra (Caltech; Assistant professor, UIUC), Danielle Tarraf (Caltech and MIT; Assistant professor, Johns Hopkins), David Thorsley (U. Washington).
Graduate students: Amir Ali Ahmadi (MIT), Asghar Aryanfar (Caltech), Julia Braman (Caltech; Robotics Engineer, NASA Johnson Space Center), Noel Du Toit (Caltech), Shashank Dwivedi (MIT), Michael Epstein (Caltech; McKinsey), Melvin Flores (Caltech; JPL), Marcella Gomez (Caltech), Mihai Florian (Caltech), Zhipu Jin (Caltech; Cisco Systems), Vanessa Jönsson (Caltech), Andrew Lamperski (Caltech), Javad Lavaei (Caltech; postdoc, Stanford), John Michael McNew (U. Washington; Toyota), Nils Napp (U. Washington), Kevin Oishi (U. Washington), Concentta Pilotto (Caltech; Assistant professor, Purdue), Steve Safarik (U. Washington), Parikshit Shah (MIT), Fayette Shaw (U. Washington), Ling Shi (Caltech; Assistant professor, HKUST), Demetri Spanos (Caltech; Visiting assistant professor, USC), Noah Stein (MIT), Peter Trautman (Caltech), Fei Wang (Caltech), Jerome White (Caltech; IBM), Matt Wu (Caltech), Nok Wongpiromsarn (Caltech; postdoc MIT/Singapore),
Undergraduates: Brian Go (Caltech), Mason Smith (Caltech).

Honors and Awards Received Pablo Parrilo, Invited Speaker, International Congress of Mathematicians (ICM 2010), Control Theory and Optimization Section, Hyderabad, India, August 2010.

AFRL Points of Contact Siva Banda, AFRL/VA, WPAFB, OH, E-mail: `Siva.Banda@wpafb.af.mil`. Met at MACCCS review, October 2010;

Air Force Interactions and Transitions (1) The Safe and Secure Systems and Software Symposium (S5) Dayton, 15 June, 2010: C. Pilotto and K. M. Chandy, "Distributed Control of Mobile Agents with Unreliable Communication: Theory and Experience with S5 Tools"; (2) 2011 National Security Scholars Conference, Organized by USAF, April 26, 2011: Participant: K. M. Chandy.

New Discoveries None to report this year.