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

30 June 2009

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. We partition the problem into three parts:

(1) *Specification*: How does the user specify continuous and discrete control policies, communications protocols and environment models (including faults)?

(2) *Design and reasoning*: How can engineers reason that their designs satisfy the specifications, including real-time computing and computation constraints, dynamics and uncertainty?

(3) *Implementation*: What are the best ways of mapping detailed designs to hardware artifacts, running on specific operating systems?

We are pursuing research on all of these parts, with linkage to industry (Boeing) and national laboratories (JPL, AFRL) as a mechanism for transitioning the research results to applications.

Accomplishments

Accomplishments over the last year include work in Lyapunov-based analysis (including sum-of-squares tools), stochastic systems (including game-theoretic approaches), distributed computing and decision making (including cooperative control) and analysis and design of hybrid control systems. We describe each of these areas separately, with summaries of recent papers forming the basis of the report.

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.

Constrained Consensus and Optimization in Multi-Agent Networks [9]. In this paper, we present distributed algorithms that can be used by multiple agents to align their estimates with a particular value over a network with time-varying connectivity. Our framework is general in that this value can represent a consensus value among multiple agents or an optimal solution of an optimization problem, where the global objective function is a combination of local agent objective functions. Our main focus is on constrained problems where the estimate of each agent is restricted to lie in a different constraint set. To highlight the effects of constraints, we first consider a constrained consensus problem and present a distributed "projected consensus algorithm" in which agents combine their local averaging operation with projection on their individual constraint sets. This algorithm can be viewed as a version of an alternating projection method with weights that are varying over time and across agents. We establish convergence and convergence rate results for the projected consensus algorithm. We next study a constrained optimization problem for optimizing the sum of local objective functions of the agents subject to the intersection of their local constraint sets. We present a distributed "projected subgradient algorithm" that involves each agent performing a local averaging operation, taking a subgradient step to minimize its own objective function, and projecting on its constraint set. We show that, with an appropriately selected step size rule, the agent estimates generated by this algorithm converge to the same optimal solution for the cases when the weights are constant and equal, and when the weights are time-varying but all agents have the same constraint set.

A Poset Framework to Model Decentralized Control Problems [11]. This paper uses partially ordered sets (posets) to study decentralized control problems arising in different settings. We show that time delayed systems with certain delay structure enables one to endow the problem with poset structure thereby allowing convex reparametrization of the problem. We show how to extend these results to spatially invariant systems. We also study the connection between posets and quadratic invariance and show that in some settings they are equivalent.

Towards Verified Distributed Software Through Refinement of Formal Archetypes [6]. This paper discusses experiments with a "model-based" approach for developing verified distributed systems in which program development is carried out by stepwise refinement: we encode, specifications and algorithm archetypes in the PVS theorem prover, carry out stepwise refinement and concomitant proofs, and obtain collections of verified algorithms encoded in PVS. Finally we transform algorithms from PVS to programs in Java. We consider a class of systems in which state spaces may be continuous and state transitions may be continuous or discrete. Coordinated multi-vehicle systems are examples of this class. Temporal properties of this class of problems are specified in terms of convergence: the system state gets arbitrarily close to a limit as time tends to infinity. Our meta-theorems for verifying convergence are extensions from control theory to a temporal logic of continuous time and state spaces.

Guaranteeing Convergence of Distributed Systems: From Specification to Implementation via Refinement [5]. This paper describes a methodology for developing and verifying a class of distributed systems using stepwise refinement and a theorem prover. The process of refinement leads to algorithms in which individual steps can be implemented atomically in a straightforward way. These algorithms are then transformed from the notation of the theorem prover to a target programming language, such as Java and Erlang. The methodology allows the system state space to be continuous. The key temporal properties that are preserved by the above refinement and transformation processes are convergence and termination. The proof techniques used are extensions of control theoretic results to temporal logic of continuous time and state spaces. We present a library of theorems and proofs to reduce the work required to develop and verify programs in this class. The applicability of the method is demonstrated by modeling and performing step-wise refinement of a collection of standard algorithms for sensor networks and multi-vehicle systems.

Specifications and Architectures of Federated Event-Driven Systems [7]. A federated event-driven system (FEDS) integrates event data pushed to it or pulled by it from multiple sites within and outside an enterprise. Performance requirements for these applications can be met by implementing applications on networks of multiprocessors. This paper describes a graph model for applications and a method of mapping the graph on to multiprocessor networks. Information flows among processors within an address space are implemented by passing pointers while information flows across address spaces are implemented by message passing. The model and implementation allows an application and the underlying hardware infrastructure to be changed relatively easily. The paper describes an application implemented in this way.

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.

Setpoint Regulation for Stochastically Interacting Robots [8]. Self-assembly of complex systems and structures is a challenging cooperative control problem involving a complex interplay between local and global dynamics and the stochastic nature of those dynamics. We have developed an integral feedback controller that regulates the average copy number of a particular assembly in a system of self-assembling 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. We prove that this controller works for a range of setpoints, and how to compute this range. Finally we demonstrate the approach on a physical testbed at the University of Washington.

Probabilistic Safety Analysis of Sensor-Driven Hybrid Automata [4]. The control programs of complex autonomous systems that have conditional branching can be modeled as linear hybrid systems. When the state knowledge is perfect, linear hybrid systems with state-based transition conditions can be verified against a specified unsafe set using existing model checking software. This paper introduces a formal method for calculating the failure probability due to state estimation uncertainty of these sensor-driven hybrid systems. Problem complexity is described and some reduction techniques for the failure probability calculation are given. An example goal-based control program is given and the failure probability for that system is calculated.

On Equilibria of Message-Passing Games [10]. This paper investigates a general class of finite dynamic games where players communicate with each other by message-passing. Messages may be delayed, received out of order, duplicated or lost, but not corrupted. The challenge posed by message-passing games is that the execution of the game is non-deterministic and, thus, the final outcome may not result in an equilibrium. We introduce a notion of termination for message-passing games which is related to self-stabilization. We present theorems relating their termination to equilibria of their corresponding alternating move games. Our results apply to both best-response games in which players always choose the best action in response to other players actions, and better-response games where players may choose any action that improves their current response.

Correlated Equilibria in Continuous Games: Characterization and Computation [12]. This paper presents several new characterizations of correlated equilibria in games with continuous utility functions. These have the advantage of being more computationally and analytically tractable than the standard definition in terms of departure functions. We use these characterizations to construct effective algorithms for approximating a single correlated equilibrium or the entire set of correlated equilibria of a game with polynomial utility functions. We then exhibit the rich structure of the set of correlated equilibria by analyzing the simplest of polynomial games, the mixed extension of matching pennies. We show that while the correlated equilibrium set is convex, the structure of its extreme points can be quite complicated. In finite games there can be a superexponential separation between the number of extreme Nash and extreme correlated equilibria. In polynomial games there can exist extreme correlated equilibria which are not finitely supported; we construct a large family of examples using techniques from ergodic theory. These examples show that in general the set of correlated equilibrium distributions of a polynomial game cannot be described by conditions on finitely many joint moments, in marked contrast to the set of Nash equilibria which is always expressible in terms of finitely many moments.

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).

Periodically Controlled Hybrid Systems: Verifying A Controller for An Autonomous Vehicle [13]. This paper introduces Periodically Controlled Hybrid Automata (PCHA) for describing a class of hybrid control systems. In a PCHA, control actions occur roughly periodically while internal and input actions, may occur in the interim changing the discrete-state or the setpoint. Based on periodicity and subtangential conditions, a new sufficient condition for verifying invariance of PCHAs is presented. This technique is used in verifying safety of the planner-controller subsystem of an autonomous ground vehicle, and in deriving geometric properties of planner generated paths that can be followed safely by the controller under environmental uncertainties.

Receding Horizon Temporal Logic Planning for Dynamical Systems [14]. This paper bridges the advances in computer science and control to allow automatic synthesis of complex dynamical systems which are guaranteed, by construction, to satisfy the desired properties even in the presence of adversary. The desired properties are expressed in the language of temporal logic. With its expressive power, a wider class of properties than safety and stability can be specified. The resulting system consists of a discrete planner which plans, in the abstracted discrete domain, a set of transitions of the system to ensure the correct behaviors and a continuous controller which continuously implements the plan. For a system with certain structure, we present an approach, based on a receding horizon scheme, to overcome computational difficulties in the synthesis of a discrete planner and allow more complex problems to be solved.

Control Program Verification for a Sample Titan Aerobot Mission [3]. Fault tolerance and safety verification of control systems are essential for the success of autonomous robotic systems. A control architecture called Mission Data System (MDS), developed at the Jet Propulsion Laboratory, takes a goal-based control approach. A software algorithm for converting goal network control programs into linear hybrid systems exists and is a bisimulation; the resulting linear hybrid system can be verified for safety in the presence of failures using existing symbolic model checkers, and thus the original goal network is verified. A substantial example control program based on a proposed mission to Titan, a moon of Saturn, is converted using the procedures discussed.

Sum of Squares 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.

Sum of Squares and Polynomial Convexity [1, 2]. A multivariate polynomial $p(x) = p(x_1, ..., x_n)$ is sos-convex if its Hessian $H(x)$ can be factored as $H(x) = M^T(x)M(x)$ with a possibly nonsquare polynomial matrix $M(x)$. It is easy to see that sos-convexity is a sufficient condition for convexity of $p(x)$. Moreover, the problem of deciding sos-convexity of a polynomial can be cast as the feasibility of a semidefinite program, which can be solved efficiently. Motivated by this computational tractability, it has been recently speculated whether sos-convexity is also a necessary condition for convexity of polynomials. In this paper, we give a negative answer to this question by presenting an explicit example of a trivariate homogeneous polynomial of degree eight that is convex but not sos-convex. Interestingly, our example is found with software using sum of squares programming techniques and the duality theory of semidefinite optimization. As a byproduct of our numerical procedure, we obtain a simple method for searching over a restricted family of nonnegative polynomials that are not sums of squares.

References

[1] A. A. Ahmadi and P. A. Parrilo. A convex polynomial that is not sos-convex. *Mathematical Programming*, 2009. Submitted.

[2] A. A. Ahmadi and P. A. Parrilo. Sum of squares and polynomial convexity. In *Proc. IEEE Control and Decision Conference*, 2009. Submitted.

[3] J. M. B. Braman and R. M. Murray. Control program verification for a sample titan aerobot mission. In *AIAA Infotech Conference*, 2009.

[4] J. M. B. Braman and R. M. Murray. Probabilistic safety analysis of sensor-driven hybrid automata. In *Hybrid Systems: Computation and Control*, 2009. Submitted.

[5] K. M. Chandy, B. Go, S. Mitra, C. Polotto, and J. White. Guaranteeing convergence of distributed systems: From specification to implementation via refinenement. *Formal Aspects of Computing*, 2009.

[6] K. M. Chandy, B. Go, S. Mitra, and J. White. Towards verified distributed software through refinement of formal archetypes. In *IFIP Working Conference on Verified Software: Workshop on Experiments*, 2008.

[7] K. M. Chandy and M. Olson. Specifications and architectures of federated event-driven systems. In *AAAI Spring Symposium on Intelligent Complex Event Processing*, 2009.

[8] N. Napp, S. Burden, and E. Klavins. Setpoint regulation for stochastically interacting robots. In *Robotics: Science and Systems*, 2009.

[9] A. Nedic, A. Ozdaglar, and P. A. Parrilo. Constrained consensus and optimization in multi-agent networks. *IEEE Transactions on Automatic Control*, 2009. Submitted.

[10] C. Pilotto and K. M. Chandy. On equilibria of message-passing games. *Distributed Computing*, 2009. Submitted.

[11] P. Shan and P. A. Parrilo. A poset framework to model decentralized control problems. In *Proc. IEEE Control and Decision Conference*, 2009. Submitted.

[12] N. D. Stein, P. A. Parrilo, and A. Ozdaglar. Correlated equilibria in continuous games: Characterization and computation. *Games and Economic Behavior*, 2009. Submitted.

[13] T. Wongpiromsarn, S. Mitra, R. M. Murray, and A. Lamperski. Periodically controlled hybrid systems: Verifying a controller for an autonomous vehicle. In *Hybrid Systems: Computation and Control*, 2009. To appear.

[14] T. Wongpiromsarn, U. Topcu, and R. M. Murray. Receding horizon temporal logic planning for dynamical systems. In *Proc. IEEE Control and Decision Conference*, 2009. Submitted.