Annual Reviews in Control 45 (2018) 1–4

Contents lists available at ScienceDirect

Annual Reviews in Control

journal homepage: www.elsevier.com/locate/arcontrol

Vision article

Advancing systems and control research in the era of ML and AI

Pramod P. Khargonekar*, Munther A. Dahleh

[a] Department of Electrical Engineering and Computer Science, University of California, Irvine, USA
[b] Department of Electrical Engineering and Computer Science Institute for Data, Systems, and Society MIT, USA

ARTICLE INFO

Article history:
Received 26 February 2018
Revised 25 March 2018
Accepted 2 April 2018
Available online 9 April 2018

Keywords:
Machine learning
Artificial intelligence
Control systems

ABSTRACT

Fields of machine learning and artificial intelligence are undergoing transformative advances and growth. This article presents a vision for the field of systems and control that simultaneously leverages these advances to more fully engage with them and spur new expansive research directions in systems and control.

Contents

How might the current and expected future advances in machine learning and artificial intelligence lead to new opportunities for the systems and control community? We have been motivated by this timely question to articulate an initial vision in this brief essay. Right at the outset, we would like to state that the discussion below is far from comprehensive. Rather, the purpose is to present a perspective and some initial thinking on how the systems and control community could engage in and help shape this emerging future more fully.

Machine learning and artificial intelligence context:

Since its inception, the field of artificial intelligence (AI) focused on understanding how computers can mimic human brains in the context of decision making. Coined by John McCarthy in 1956, AI is a very general field covering disparate topics such as search, planning, reasoning, learning, natural language processing, perception, vision, etc. Machine learning, coined by Arthur Samuel, focuses on achieving AI through training and learning, and has its roots in statistical learning theory. Over the last decade, great advances have been made in AI and ML in several dimensions: theory, application, and implementation.

Specifically in the context of ML, deep learning architectures, algorithms and techniques have created powerful tools to learn representations of large volumes of data in multiple layers of representation (LeCun, Bengio, & Hinton, 2015). These tools appear to be very successful in learning complex functions and discovering intricate structures in high-dimensional data. They have shown superior performance in image and speech recognition and are being applied in a wide variety of problems: drug discovery, particle physics, astronomy, and biomedicine. While it is difficult to summarize (and beyond the purpose and scope of this paper,) all advancements in ML, there are several directions that are particularly relevant to the subsequent discussion.

1. High dimensional statistics that focuses on computational and statistical issues pertaining to learning high dimensional sparse sets of parameters from observations (Tropp, 2015). This development ties well with research areas in compressive sensing, but expands the results to include more elaborate sparse models such as sparse graphs.
2. Online learning which addresses sequential learning and decision making in bandit problems (Rakhlin, Sridharan, & Tewari, 2015). Developments in this direction resulted in different algorithms under different information structures that can guarantee asymptotic optimality. Regret-based algorithms are one outcome of these developments.
3. Discovery of structural and latent variables using spectral and tensor methods (Anandkumar, Ge, Hsu, Kakade, & Telgarsky, 2014). Such an approach became popular in the context of topic modeling and mixtures of Gaussian models where the underlying mixture is not a priori known.

* Corresponding author.
E-mail address: pramod.khargonekar@uci.edu (P.P. Khargonekar).

https://doi.org/10.1016/j.arcontrol.2018.04.001
1367-5788/

4. Optimization for ML including the exploitation of randomness in the context of maximum likelihood learning for non-convex network models (Zwiernik, Uhler, & Richards, 2017) and stochastic gradient algorithms in the context of deep learning (Hardt, Recht, & Singer, 2016; Rakhlin, Raginsky, & Telgarsky, 2017).

Advancements in these areas have substantially influenced many application domains.

More broadly, the confluence of insights and techniques from neuroscience, cognitive science, reinforcement learning (RL), and deep learning (DL) has led to very impressive progress in ML and AI with amazing achievements in championship games and demonstration of human level control by an artificial agent (Hassabis, Kumaran, Summerfield, & Botvinick, 2017; Mnih et al., 2015). Increasing computational power (thanks to Moore's Law progress), availability of large amounts of data, and development of more effective algorithms have been critical to many of these successes and will be increasingly even more important to continuing progress (Dean, Patterson, & Young, 2018; Simonite, 2017). Driven by the excitement of progress and potential for major benefits, there is a flood of interest, and corresponding investments, in ML and AI from the academic, industrial and government sectors (Bughin et al., 2017). Yet, there are significant weaknesses and issues that need to be resolved for future progress. These include insufficient and incomplete theoretical foundations, need for large amounts of data, lack of robustness and vulnerability to adversarial attacks, lack of transparency and explainability, biases resulting from algorithms and data, etc.

It is our position that AI should entail some sort of learning combined with decision making. However, in many application areas, AI refers to decision making more broadly. For many of these AI systems, their ability to learn, especially in real-time, is quite limited. As Brooks observes in his very interesting critique of exaggerated AI predictions (Brooks, 2017), "Today's machine learning is not at all the sponge-like learning that humans engage in, making rapid progress in a new domain without having to be surgically altered or purpose-built. ... When humans play a game, a small change in rules does not throw them off. Not so for AlphaGo or Deep Blue." While the latest AI systems such as AlphaGo Zero (Silver et al., 2017) exhibit certain impressive learning abilities, it is far from clear whether these systems can learn to adapt to and deal with rapid and unforeseen changes in the environment.

Control systems: Control systems have a deep, broad and strong base of foundational knowledge developed over the last 60 years with major emphasis on decision making under uncertainty. Dynamic systems modeling, structural properties, model reduction, identification, stability, feedback, optimality, robustness, adaptation, fault tolerance, and architecture have been among the central concerns on the theoretical side. These issues have been explored in a wide variety of settings: linear, nonlinear, stochastic, hybrid, distributed, supervisory, and others. Applications have been wide ranging: aerospace, automotive, manufacturing, chemical process, energy, power, transportation, etc. While there is a very rich history, the future is just as promising as there are a multitude of directions for future theoretical and applications research (Lamnabhi-Lagarrigue et al., 2017). Despite all the progress in various subfields of systems and control, much remains to be done to satisfactorily address control of large, complex, distributed dynamical systems under rapid changes in the environment and high levels of uncertainty.

Future This is truly an opportune moment to develop a forward looking vision that can inspire talented researchers for the next decade or longer. On the one hand, a major goal of AI is to build machines that can learn and think for themselves (Lake, Ullman, Tenenbaum, & Gershman, 2017), including having imagination, reasoning, planning, etc. On the other hand, we have a rich body of knowledge in control systems. The field of control can both benefit from and influence the ongoing revolutionary advances in ML and AI. These advances in ML and AI are going to be driven by the large increases in computation power and data, intense interest across the world, and large investments in these fields across academic, industrial and government organizations. By leveraging these ongoing trends and advances in ML/AI, we can aim to have significantly more powerful and versatile control systems. For this, we would need to define specific goals that are currently unachievable with existing control techniques but could potentially be achieved by leveraging ML/AI advances. Such goals would likely be driven by major application areas for control. They would have implications and opportunities for theoretical developments in control. On the other side, we can identify ideas, tools and techniques from control systems that have the potential to advance AI in its quest of building machines that learn and think for themselves. Examples include principles and techniques from robust and adaptive control, stochastic control, dynamic programming, system identification, model predictive control, decentralized and distributed control, and agent based control.

Of course, there are historic connections between learning, artificial intelligence, and control systems going back to the 60's. Research fields such as intelligent control and neural networks for control arose from these long standing connections. Closer to the recent developments in ML and AI that are the main focus of this paper, there are deep connections between RL (Sutton & Barto, 1998) and stochastic control (Bertsekas & Tsitsiklis, 1995). There are more recent and much less investigated connections between learning in sensorimotor neural systems (Grush, 2004; Wolpert, Ghahramani, & Flanagan, 2001) and controls, e.g., the role of forward and inverse models for control in the central nervous system, emulation theory of representation that builds on control and Kalman filtering, etc. More generally, very recent developments in neuroscience such as the free energy principle and a unified brain theory (Friston, 2010) are deeply connected with central ideas in systems and control but have received not much attention in controls community and where further explorations are likely to be very fruitful.

In a more speculative and somewhat controversial longer-term direction, while there is acceptance within the AI community that rich internal models are critical to human like learning and decision making and that the learning processes must be informed and constrained by prior knowledge, there is considerable debate within the AI community on whether such internal models should be configured by human designers or should be learned by the AI agent de novo (Botvinick et al., 2017; Lake et al., 2017). (Such debates are not far from the Chomsky-Skinner debate which articulated a fundamental dichotomy in understanding language acquisition; one side that is based on the learning of a fixed architecture in the brain (Chomsky) and the other that is based on statistical interpretation of the relationships between the past and present behavior (Skinner) (Chomsky, 1959; Skinner, 2014).) Debates around these questions in AI are far from settled and the research field is rich with open questions and may turn out to offer new opportunities, in view of the centrality of model building aspects in the debates, for systems and control community to engage, contribute, and benefit.

It is worthwhile emphasizing that a substantial part of control theory focuses on fundamental limits of stability and performance. For example, the theory addresses questions such as characterizing the minimal information needed about a process to control it (say to achieve a desired objective). At the same time, statistical learning theory (both standard and high dimensional) focuses on obtaining information-theoretic limits of achievable model accuracy from data. Can these two seemingly disparate paradigms be

combined to provide rigorous fundamental limits of certain AI systems? More so, can such understanding improve the algorithmic aspects of designing AI systems?

Potential research directions: There is potentially a very rich and attractive research agenda that arises from the above considerations. What will turn out to be the most important promising research directions will only become clear with the passage of time as research community explores various possibilities and novel discoveries come into focus. Some initial ideas for interesting research explorations are briefly outlined below:

- Traditionally, control systems analysis and design has been based on detailed mathematical models of the system and the environment and with fairly well-understood sources of uncertainty. These models are typically described using differential equations, discrete-event formalisms, Markov processes, etc. Construction of such models requires highly specific scientific and engineering knowledge, data, and domain expertise. By contrast, ML and (some) AI methods aim to learn models (and control actions) directly from data and experiments. Clearly, in areas where detailed traditional control-oriented models are feasible and have already been developed, there is modest scope for ML and AI techniques such as use of deep neural networks for function approximation or rules in discrete-event systems. However, a much larger opportunity arises in areas where (a) such detailed, mechanistic mathematical models do not exist, and/or (b) where performance goals are described at a high level, and/or (c) where the amount of uncertainty is significantly greater with unknown sources, and/or (d) where the control goals and tasks have high diversity. In such contexts, how can we rethink and re-conceptualize the role of models in control systems in light of what has been learnt in ML and AI in recent years? The big opportunity here for the research community is to create new problem formulations where background foundational knowledge from control might be creatively mixed with new paradigms in ML and AI to open new application domains or extend well beyond current performance objectives, especially for rapid changes in the environment and high levels of uncertainty. Application domains for systems and control are numerous and diverse (Lamnabhi-Lagarrigue et al., 2017). In many of these domains, e.g., transportation, aerospace, biomedical, manufacturing, energy, to name a few, the above-mentioned considerations are applicable. Thus, the potential for future research along this line of thinking is very high.
  One example that demonstrates this interaction is the relationship between the recently developed spectral methods for machine learning and the classical model reduction techniques that are widely explored in the context of dynamic systems' simulation and control. In the absence of prior characterizations of model sparsity, estimating a low dimensional model directly from data can have powerful generalization properties. Exploring such approaches for unstructured models (e.g., Hidden Markov Models, Deep Networks) will allow for a principled approach in designing algorithms for data-driven decision making.
- Neuroscience and cognitive science insights have been key drivers in certain major breakthroughs in AI (Hassabis et al., 2017). The key goal there has been to build machines that can learn and think for themselves (Lake et al., 2017). Historically, cybernetics was conceived by Wiener (1961) as "the scientific study of control and communication in the animal and the machine". Over time, this connection between control and cybernetics did not develop as fully as the mathematical control theory paradigm (Kalman, Falb, & Arbib, 1969). Can we leverage the new insights at the confluence of neuroscience, cognitive science, reinforcement learning, and AI to conceptualize new architectures for versatile, intelligent and adaptive controllers that work across large diverse domains with improving performance while maintaining safety? Here the big opportunity is to go significantly beyond existing frameworks and paradigms for adaptive control and realize the vision behind Wiener's original cybernetics ideas thereby achieving much higher levels of autonomy, robustness, and adaptive performance.
  Stepping back to specific applications for concreteness, consider the problem of designing neural prosthetics (e.g., to compensate for spinal cord injuries). Here we can greatly benefit from the development of neuromorphic computing that integrates well into effective control architectures. Such architectures should embed biologically-sound signal representations to allow describing high-level objectives and to translate them to specific control strategies.
- Recent work in AI has led to very impressive results on "human-level control" using an artificial agent that incorporates reinforcement learning and deep Q-network on a large variety of video games (Mnih et al., 2015). A key challenge here is combine high-dimensional sensory inputs into learning control actions. Thus, the ability of the artificial agent to achieve performance that exceeds all prior algorithms and a level that is comparable to professional human tester can be viewed as an achievement in control performance. This advance in AI creates an opportunity to examine the analysis and design of such artificial agents from a control theory perspective. A close collaboration between reinforcement learning, artificial intelligence, and control theory communities might lead to important advances in theory as well as applications.
  In the context of smart services (e.g., transportation, power), humans constitute an essential component of the system. Mechanism design aims to create incentive compatible strategies that attempts to drive human behavior towards a desirable equilibrium. The absence of mechanistic models describing how people behave in response to incentives highlights the importance of real-time learning and adaptations for such systems. This presents another opportunity for bringing together cognitive science and game theory to address questions and challenges pertaining to incentivizing human behavior.
- While there have been impressive advances in deep learning, many aspects remain only partially understood. For example, some recent results show that deep neural networks easily fit *random* labels (Zhang, Bengio, Hardt, Recht, & Vinyals, 2016). This key finding along with additional reasoning leads the authors of Zhang et al. (2016) to state, "... poses a conceptual challenge to statistical learning theory as traditional measures of model complexity struggle to explain the generalization ability of large artificial neural networks". Thus, there is considerable gap in understanding why deep neural networks have small generalization error in many real world applications. Can methods and tools from systems and control theory offer new analytical perspectives and understanding of this empirical fact? In a related direction, it is now well-known (Dauphin et al., 2014) that saddle points in high-dimensional non-convex optimization are a critical barrier in optimization and training of deep neural networks. There is thus an opportunity for systems and control theory community to contribute innovative non-convex optimization solutions to this saddle point problem.
- It is known, and evidence continues to grow, that many of the machine learning algorithms are not *robust* (Szegedy et al., 2013). For example, image recognition algorithms using deep neural networks can lead to wrong classification if the image is altered in even small ways. This lack of robustness is potentially a major problem, especially if there are adversaries who intend to cause cyber-physical sabotage of intelligent autonomous sys-

tems (Hein & Andriushchenko, 2017). In order for a system to learn and make good decisions in real time, it has to keep a good account of the part of the process it is *not* able to model (this includes unexplored dynamics and adversaries). Estimating such uncertainty is rooted in the model selection process which many AI systems are envisioned to choose on the fly. What are the opportunities to use insights from robust, adaptive stochastic control to advance machine learning and artificial intelligence by addressing these limitations?

References

Anandkumar, A., Ge, R., Hsu, D., Kakade, S. M., & Telgarsky, M. (2014). Tensor decompositions for learning latent variable models. *Journal of Machine Learning Research, 15*, 2773–2832.

Bertsekas, D. P., & Tsitsiklis, J. S. (1995). *Dynamic programming and optimal control*. Athena scientific Belmont, MA.

Botvinick, M., Barrett, D. G., Battaglia, P., de Freitas, N., Kumaran, D., Leibo, J. Z., et al. (2017). Building machines that learn and think for themselves. *Behavioral and Brain Sciences, 40*, 26–28.

Brooks, R. (2017). The seven deadly sins of AI predictions. https://www.technologyreview.com/s/609048/the-seven-deadly-sins-of-ai-predictions/.

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., Henke, N., & Trench, M. (2017). Artificial intelligence–the next digital frontier. https://www.mckinsey.de/files/170620_studie_ai.pdf.

Chomsky, N. (1959). A review of bf skinner's verbal behavior. *Language, 35*, 26–58.

Dauphin, Y. N., Pascanu, R., Gulcehre, C., Cho, K., Ganguli, S., & Bengio, Y. (2014). Identifying and attacking the saddle point problem in high-dimensional non–convex optimization. In *Advances in neural information processing systems* (pp. 2933–2941).

Dean, J., Patterson, D., & Young, C. (2018). A new golden age in computer architecture: Empowering the machine learning revolution. *IEEE Micro, PP*. 1–1

Friston, K. (2010). The free-energy principle: a unified brain theory? *Nature Reviews Neuroscience, 11*(2), 127–138.

Grush, R. (2004). The emulation theory of representation: Motor control, imagery, and perception. *Behavioral and brain sciences, 27*(3), 377–396.

Hardt, M., Recht, B., & Singer, Y. (2016). Train faster, generalize better: Stability of stochastic gradient descent. In *International Conference on Machine Learning* (pp. 1225–1234).

Hassabis, D., Kumaran, D., Summerfield, C., & Botvinick, M. (2017). Neuroscience-inspired artificial intelligence. *Neuron, 95*(2), 245–258.

Hein, M., & Andriushchenko, M. (2017). Formal guarantees on the robustness of a classifier against adversarial manipulation. In *Advances in neural information processing systems* (pp. 2263–2273).

Kalman, R. E., Falb, P. L., & Arbib, M. A. (1969). *Topics in mathematical system theory*. McGraw-Hill New York.

Lake, B. M., Ullman, T. D., Tenenbaum, J. B., & Gershman, S. J. (2017). Building machines that learn and think like people. *Behavioral and Brain Sciences, 40*, 1–72.

Lamnabhi-Lagarrigue, F., Annaswamy, A., Engell, S., Isaksson, A., Khargonekar, P., Murray, R. M., et al. (2017). Systems & control for the future of humanity, research agenda: Current and future roles, impact and grand challenges. *Annual Reviews in Control, 43*, 1–64.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444.

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., et al. (2015). Human-level control through deep reinforcement learning. *Nature, 518*(7540), 529–533.

Rakhlin, A., Raginsky, M., & Telgarsky, M. (2017). Non-convex learning via stochastic gradient langevin dynamics: A nonasymptotic analysis. *Conference on Learning Theory*, 1674–1703.

Rakhlin, A., Sridharan, K., & Tewari, A. (2015). Online learning via sequential complexities. *Journal of Machine Learning Research, 16*, 155–186.

Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., et al. (2017). Mastering the game of go without human knowledge. *Nature, 550*(7676), 354–359.

Simonite, T. (2017). How AI Can Keep Accelerating After Moore's Law. https://www.technologyreview.com/s/607917/how-ai-can-keep-accelerating-after-moores-law/.

Skinner, B. F. (2014). *Verbal behavior*. B.F. Skinner Foundation.

Sutton, R. S., & Barto, A. G. (1998). *Reinforcement Learning: An Introduction*. MIT press Cambridge.

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. arXiv:1312.6199.

Tropp, J. (2015). An introduction to matrix concentration inequalities. *Foundations and Trends® in Machine Learning, 8*, 1–230.

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machine*. MIT Press.

Wolpert, D. M., Ghahramani, Z., & Flanagan, J. R. (2001). Perspectives and problems in motor learning. *Trends in Cognitive Sciences, 5*(11), 487–494.

Zhang, C., Bengio, S., Hardt, M., Recht, B., & Vinyals, O. (2016). Understanding deep learning requires rethinking generalization. arXiv:1611.03530.

Zwiernik, P., Uhler, C., & Richards, D. (2017). Maximum likelihood estimation for linear gaussian covariance models. *Journal of the Royal Statistical Society: Series B, 79*, 1269–1292.