Generative Learning and Agent-Based Simulation for Synthesis of Complex System Datasets

Recent years have seen an explosion of available data from real-world complex systems (e.g., transportation, healthcare, commerce, financial markets) that characterizes agent behavior and collective system properties over time. Despite their great potential to inform trustworthy and beneficial AI, high-quality datasets that can directly help to address problems of interest often do not exist, due to three major challenges:

(a) The release of agent-level data can reveal sensitive information about individuals in the system.
Example: in a dataset with human mobility traces, four spatio-temporal points are sufficient to uniquely identify 95% of the individuals within the spatial resolution of an antenna [1].

(b) Data generally does not come labeled, and thus often requires expensive annotation efforts to support research questions of interest.
Example: intent recognition algorithms are mostly trained on handcrafted libraries under simulated environments, due to the unobservability of intent in naturally collected data [2].

(c) Though data of relevant situations may exist, (data regarding) direct experience for the issue at hand is little.
Example: historical data alone does not indicate how agents would react to a new policy or circumstance [3].

My research objective is to overcome these challenges, and develop algorithms to generate high-fidelity synthetic data that (1) realistically captures system patterns and agent behavior observed in the real world, and (2) is customized to serve a particular data usage purpose. For example, consider generating a diverse set of driver and rider behaviors to help optimize the design of ridesharing platforms, or simulating sequences of e-commerce transactions to facilitate training a detector for feedback manipulation.

Intellectual Merit Recent developments in *deep generative models* [4, 5, 6] have demonstrated success in generating highly-realistic images and texts, even with controlled attributes (e.g., human faces with glasses [7], sentences with desired sentiments [8]). However, these developed techniques may not suffice to generate complex-system data, such as that reflecting multi-agent interactions, especially when labeled real data does not exist in large quantity. *Agent-based modeling*, on the other hand, directly specifies agent behaviors through decision-making rules (or *policy* in reinforcement learning), and system properties through the interaction of agents [9]. Moreover, labels can be associated with simulated data by design. For example, we can tag a sequence of e-commerce transactions made by a manipulation agent as malicious, since they are devised (or learned) to achieve the manipulation objective (e.g., changing system recommendations even in the absence of normal purchases and consumer feedback). However, simulators may not capture real-world scenarios with high fidelity, and learning algorithms developed from simulated data may overfit to artifacts and fail to generalize.

This research explores techniques to combine generative models with agent-based models for generating realistic synthetic data of large-scale multi-agent systems that meets specified attributes of interest (e.g., trip patterns after a sporting event, or manipulation of a recommender system). The goal is to generate high-quality data both in the system aggregate and at the agent-level and to solve specific challenges faced by the data use case.

The use of an agent-based model together with a generative model serves two major benefits. *First*, it provides information about a behavioral attribute of interest (e.g., traffic patterns or manipulation traces), by simulating appropriate world environments in case of insufficient labeled real data. This conditioning information can be then integrated into the generative model (e.g., in a similar fashion as conditional GANs [10]). *Second*, it helps to quantify the extent to which the generated data conforms to required behavioral attributes, modifying the generator's loss function to preserve these attributes. The generative model, on the other hand, provides the flexibility to meet particular needs, by adopting a combination of different, application-specific loss terms. For example, consider incorporating *differential privacy* [11] into the loss design of a generator to preserve agent privacy, making use of feedback from the simulator to conform with conditional attributes, or leveraging the *reward* from a decision-making algorithm to adversarially generate new circumstances that are considered hard.

Broader Impacts The techniques developed here will enable high-fidelity data sharing, allowing data owners to prepare simulators of actual systems that are customized to the particular needs of AI or analytics challenges, while avoiding overfitting to one particular data set and protecting privacy. If successful, the project will contribute to bridging the gap between simulators and real-world applications, introducing algorithms that have achieved empirical successes on smaller datasets to a more complex, realistic, but trainable playground. More broadly, high-quality simulators open up the possibility to break away from common scenarios encountered (through generating rare events) and provide challenging environments in which to develop trustworthy AI systems. This can help decision makers to develop reliable and robust algorithms that are effective in the real world.

This document elaborates milestone tasks that I plan to achieve for the system-level and agent-level data generation, proposes evaluation methods to assess these tasks, and describes potential data sources that can be used to train and test the generative algorithms.

Research Plan I plan to start with *generating high-fidelity data in the system aggregate*. In preliminary work [12], my coauthors and I have demonstrated the effectiveness of using a Wasserstein GAN [13] to generate realistic order streams of a stock market. A natural next step is to augment this generator with a well-defined conditioning attribute, such as a market shock. These kinds of shocks have been characterized in agent-based models in prior literature [14, 15], and a small set of such cases may also be collected from stock market data (such as incidents happened during March 2020). The goal is to extract latent features that can represent a shock from a combination of simulated and observed data, using this to provide conditioning information for the generative model.

Generating data series in the system aggregate can be viewed as generating dynamic environments, where a strategic agent will rationally behave to maximize utility. I am interesting in using the generative model to craft complex-system environments that are considered "hard" by the agent, posing a game between a decision-making agent and the environment generator. Pinto et al. showed in OpenAI Gym's environments [17] that policy learning can be more robust and stable when agents have been exposed to adversarial settings [16]. More broadly, such process generates data regarding direct experience for different (unseen) environments, providing a way to foresee strategic behavior of agents in novel circumstances.

I plan to investigate *generating synthetic data at the agent-level*, by considering the two cases of whether descriptive statistics about each individual agent are or are not available (learnable). For the identified case, consider user-level data from ridesharing platforms, where agent preferences can be inferred from ride history. A suitable task here would be to protect the privacy of ride traces (e.g., by employing differential privacy techniques within the context of a generative model), while preserving the original preferences of agents (e.g., trajectories of users who prefer Uber Express Pool should still reflect a hybrid of walking and ridesharing).

For the non-identified case, the task is to calibrate labeled data from an agent-based model to (unlabeled) agent-level data in the real world. My preliminary work in the context of stock market data showcases the possibility of using a generator to refine simulated manipulation actions, such that the adapted sequence of actions mimics a targeted normal activity pattern, while preserving some manipulation effects [18]. Along this line, I plan to substitute the targeted distribution with (a selective) set of unlabeled data to produce labeled realistic agent behavior. Finally, an ambitious step is to look to design a simulator where agents interact with each other to collectively produce a realistic system property, while still (individually) adhering to their decision-making modules.

Research milestones proposed here build on my research experience in game-theoretic reasoning and machine learning, and extends to relevant new areas, including differential privacy and multi-agent reinforcement learning.

Evaluation Plan Success will mean techniques that are able to generate synthetic datasets that (1) resemble real-world data, and (2) meet a specified attribute requirement to support further usage. I plan to quantitatively measure (1) by proposing domain-specific metrics and adopting techniques developed to evaluate generative models [19] and simulators [20]. One potential way to evaluate (2) in the laboratory is to understand how an algorithm could benefit from including customized synthetic data in its training process. In practice, I would like to seek collaboration with both data providers (e.g., ridesharing platforms, financial exchanges) and data users (e.g., researchers) to assess the usability, credibility, and trustworthiness of generated data.

Data Sources I will pursue data sources that cover different real-world complex systems and capture data at various granularity to facilitate accomplishing the research goal. Below I describe several available datasets:

(1) Trip data on Uber and other for-hire vehicle (FHV) in New York City[1] which includes around 20 million trip-level data, and for each contains a trip time, pick-up and drop-off location, and FHV number.
(2) OneTick time-series database[2] which includes order-by-order data on a range of stock markets. Each order can be tracked throughout its life-cycle, and features a buy or sell type, limit price, number of shares, and timestamp.
(3) Human subjects data from a crowdsourcing project on cooperative AI in Atari environments.

CISE research area: Robust Intelligence (RI) under Information and Intelligent Systems (IIS).

[1] `www.kaggle.com/fivethirtyeight/uber-pickups-in-new-york-city`
[2] `https://www.onetick.com/`

References

[1] Yves-Alexandre De Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. *Scientific reports*, 3(1376), 2013.

[2] Gita Sukthankar, Christopher Geib, Hung Hai Bui, David Pynadath, and Robert P. Goldman. *Plan, Activity, and Intent Recognition: Theory and Practice*. Morgan Kaufmann Publishers Inc., 2014.

[3] Judea Pearl. *Causality: Models, Reasoning, and Inference*. Cambridge University Press, 2009.

[4] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In *28th International Conference on Neural Information Processing Systems (NIPS)*, 2014.

[5] Diederik P. Kingma and Max Welling. Auto-encoding variational bayes. In *2nd International Conference on Learning Representations (ICLR)*, 2014.

[6] Aäron Van Den Oord, Nal Kalchbrenner, and Koray Kavukcuoglu. Pixel recurrent neural networks. In *33rd International Conference on International Conference on Machine Learning (ICML)*, 2016.

[7] Alec Radford, Luke Metz, and Soumith Chintala. Unsupervised representation learning with deep convolutional generative adversarial networks. In *4th International Conference on Learning Representations (ICLR)*, 2016.

[8] Lajanugen Logeswaran, Honglak Lee, and Samy Bengio. Content preserving text generation with attribute controls. In *32nd International Conference on Neural Information Processing Systems (NeurIPS)*, 2018.

[9] Eric Bonabeau. Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences*, 99(3):7280–7287, 2002.

[10] Mehdi Mirza and Simon Osindero. Conditional generative adversarial nets. *arXiv preprint*, arXiv:1411.1784, 2014.

[11] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography*, pages 265–284, 2006.

[12] Junyi Li, Xintong Wang, Yaoyang Lin, Arunesh Sinha, and Michael P. Wellman. Generating realistic stock market order streams. In *34th International Conference on Artificial Intelligence (AAAI)*, 2020.

[13] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *34th International Conference on Machine Learning (ICML)*, 2017.

[14] Dimitris Bertsimas and Andrew W. Lo. Optimal control of execution costs. *Journal of Financial Markets*, 1 (1):1–50, 1998.

[15] Erik Brinkman. *Understanding Financial Market Behavior through Empirical Game-Theoretic Analysis*. PhD thesis, The University of Michigan, Ann Arbor, 2018.

[16] Lerrel Pinto, James Davidson, Rahul Sukthankar, and Abhinav Gupta. Robust adversarial reinforcement learning. In *34th International Conference on Machine Learning (ICML)*, 2017.

[17] Greg Brockman, Vicki Cheung, Ludwig Pettersson, Jonas Schneider, John Schulman, Jie Tang, and Wojciech Zaremba. OpenAI gym. *arXiv preprint*, arXiv:1606.01540, 2016.

[18] Xintong Wang and Michael P. Wellman. Market manipulation: An adversarial learning framework for detection and evasion. In *29th International Joint Conference on Artificial Intelligence (IJCAI)*, 2020.

[19] Ali Borji. Pros and cons of GAN evaluation measures. *Computer Vision and Image Understanding*, 179:41–65, 2019.

[20] R G Sargent. Verification and validation of simulation models. *Journal of Simulation*, 7(1):12–24, 2013.