Thu 2024.03.28

Do LLM Agents Have Regret? A Case Study in Online Learning and Games

Chanwoo Park, Xiangyu Liu, Asuman Ozdaglar, Kaiqing Zhang

Large language models (LLMs) have been increasingly employed for (interactive) decision-making, via the development of LLM-based autonomous agents. Despite their emerging successes, the performance of LLM agents in decision-making has not been fully investigated through quantitative metrics, especially in the multi-agent setting when they interact with each other, a typical scenario in real-world LLM-agent applications. To better understand the limits of LLM agents in these interactive environments, we propose to study their interactions in benchmark decision-making settings in online learning and game theory, through the performance metric of \emph{regret}. We first empirically study the {no-regret} behaviors of LLMs in canonical (non-stationary) online learning problems, as well as the emergence of equilibria when LLM agents interact through playing repeated games. We then provide some theoretical insights into the no-regret behaviors of LLM agents, under certain assumptions on the supervised pre-training and the rationality model of human decision-makers who generate the data. Notably, we also identify (simple) cases where advanced LLMs such as GPT-4 fail to be no-regret. To promote the no-regret behaviors, we propose a novel \emph{unsupervised} training loss of \emph{regret-loss}, which, in contrast to the supervised pre-training loss, does not require the labels of (optimal) actions. We then establish the statistical guarantee of generalization bound for regret-loss minimization, followed by the optimization guarantee that minimizing such a loss may automatically lead to known no-regret learning algorithms. Our further experiments demonstrate the effectiveness of our regret-loss, especially in addressing the above ``regrettable'' cases.

link: http://arxiv.org/abs/2403.16843v1

GreeDy and CoDy: Counterfactual Explainers for Dynamic Graphs

Zhan Qu, Daniel Gomm, Michael Färber

Temporal Graph Neural Networks (TGNNs), crucial for modeling dynamic graphs with time-varying interactions, face a significant challenge in explainability due to their complex model structure. Counterfactual explanations, crucial for understanding model decisions, examine how input graph changes affect outcomes. This paper introduces two novel counterfactual explanation methods for TGNNs: GreeDy (Greedy Explainer for Dynamic Graphs) and CoDy (Counterfactual Explainer for Dynamic Graphs). They treat explanations as a search problem, seeking input graph alterations that alter model predictions. GreeDy uses a simple, greedy approach, while CoDy employs a sophisticated Monte Carlo Tree Search algorithm. Experiments show both methods effectively generate clear explanations. Notably, CoDy outperforms GreeDy and existing factual methods, with up to 59\% higher success rate in finding significant counterfactual inputs. This highlights CoDy's potential in clarifying TGNN decision-making, increasing their transparency and trustworthiness in practice.

link: http://arxiv.org/abs/2403.16846v1

Multiple Object Tracking as ID Prediction

Ruopeng Gao, Yijun Zhang, Limin Wang

In Multiple Object Tracking (MOT), tracking-by-detection methods have stood the test for a long time, which split the process into two parts according to the definition: object detection and association. They leverage robust single-frame detectors and treat object association as a post-processing step through hand-crafted heuristic algorithms and surrogate tasks. However, the nature of heuristic techniques prevents end-to-end exploitation of training data, leading to increasingly cumbersome and challenging manual modification while facing complicated or novel scenarios. In this paper, we regard this object association task as an End-to-End in-context ID prediction problem and propose a streamlined baseline called MOTIP. Specifically, we form the target embeddings into historical trajectory information while considering the corresponding IDs as

in-context prompts, then directly predict the ID labels for the objects in the current frame. Thanks to this end-to-end process, MOTIP can learn tracking capabilities straight from training data, freeing itself from burdensome hand-crafted algorithms. Without bells and whistles, our method achieves impressive state-of-the-art performance in complex scenarios like DanceTrack and SportsMOT, and it performs competitively with other transformer-based methods on MOT17. We believe that MOTIP demonstrates remarkable potential and can serve as a starting point for future research. The code is available at https://github.com/MCG-NJU/MOTIP.

link: http://arxiv.org/abs/2403.16848v1

Can ChatGPT predict article retraction based on Twitter mentions?

Er-Te Zheng, Hui-Zhen Fu, Zhichao Fang

Detecting problematic research articles timely is a vital task. This study explores whether Twitter mentions of retracted articles can signal potential problems with the articles prior to retraction, thereby playing a role in predicting future retraction of problematic articles. A dataset comprising 3,505 retracted articles and their associated Twitter mentions is analyzed, alongside 3,505 non-retracted articles with similar characteristics obtained using the Coarsened Exact Matching method. The effectiveness of Twitter mentions in predicting article retraction is evaluated by four prediction methods, including manual labelling, keyword identification, machine learning models, and ChatGPT. Manual labelling results indicate that there are indeed retracted articles with their Twitter mentions containing recognizable evidence signaling problems before retraction, although they represent only a limited share of all retracted articles with Twitter mention data (approximately 16%). Using the manual labelling results as the baseline, ChatGPT demonstrates superior performance compared to other methods, implying its potential in assisting human judgment for predicting article retraction. This study uncovers both the potential and limitation of social media events as an early warning system for article retraction, shedding light on a potential application of generative artificial intelligence in promoting research integrity.

link: http://arxiv.org/abs/2403.16851v1

Towards Explainability in Legal Outcome Prediction Models

Josef Valvoda, Ryan Cotterell

Current legal outcome prediction models - a staple of legal NLP - do not explain their reasoning. However, to employ these models in the real world, human legal actors need to be able to understand their decisions. In the case of common law, legal practitioners reason towards the outcome of a case by referring to past case law, known as precedent. We contend that precedent is, therefore, a natural way of facilitating explainability for legal NLP models. In this paper, we contribute a novel method for identifying the precedent employed by legal outcome prediction models. Furthermore, by developing a taxonomy of legal precedent, we are able to compare human judges and our models with respect to the different types of precedent they rely on. We find that while the models learn to predict outcomes reasonably well, their use of precedent is unlike that of human judges.

link: http://arxiv.org/abs/2403.16852v1

An Expert is Worth One Token: Synergizing Multiple Expert LLMs as Generalist via Expert Token Routing

Ziwei Chai, Guoyin Wang, Jing Su, Tianjie Zhang, Xuanwen Huang, Xuwu Wang, Jingjing Xu, Jianbo Yuan, Hongxia Yang, Fei Wu, Yang Yang

We present Expert-Token-Routing, a unified generalist framework that facilitates seamless integration of multiple expert LLMs. Our framework represents expert LLMs as special expert tokens within the vocabulary of a meta LLM. The meta LLM can route to an expert LLM like generating new tokens. Expert-Token-Routing not only supports learning the implicit expertise of expert LLMs from existing instruction dataset but also allows for dynamic extension of new expert LLMs in a plug-and-play manner. It also conceals the detailed collaboration process from the user's perspective, facilitating interaction as though it were a singular LLM. Our framework outperforms

various existing multi-LLM collaboration paradigms across benchmarks that incorporate six diverse expert domains, demonstrating effectiveness and robustness in building generalist LLM system via synergizing multiple expert LLMs.

link: http://arxiv.org/abs/2403.16854v1

Semantic-Aware Remote Estimation of Multiple Markov Sources Under Constraints

Jiping Luo, Nikolaos Pappas

This paper studies semantic-aware communication for remote estimation of multiple Markov sources over a lossy and rate-constrained channel. Unlike most existing studies that treat all source states equally, we exploit the semantics of information and consider that the remote actuator has different tolerances for the estimation errors of different states. We aim to find an optimal scheduling policy that minimizes the long-term state-dependent costs of estimation errors under a transmission frequency constraint. We theoretically show the structure of the optimal policy by leveraging the average-cost Constrained Markov Decision Process (CMDP) theory and the Lagrangian dynamic programming. By exploiting the optimal structural results, we develop a novel policy search algorithm, termed intersection search plus relative value iteration (Insec-RVI), that can find the optimal policy using only a few iterations. To avoid the ``curse of dimensionality'' of MDPs, we propose an online low-complexity drift-plus-penalty (DPP) scheduling algorithm based on the Lyapunov optimization theorem. We also design an efficient average-cost Q-learning algorithm to estimate the optimal policy without knowing a priori the channel and source statistics. Numerical results show that continuous transmission is inefficient, and remarkably, our semantic-aware policies can attain the optimum by strategically utilizing fewer transmissions by exploiting the timing of the important information.

link: http://arxiv.org/abs/2403.16855v1

XAIport: A Service Framework for the Early Adoption of XAI in AI Model Development

Zerui Wang, Yan Liu, Abishek Arumugam Thiruselvi, Abdelwahab Hamou-Lhadj

In this study, we propose the early adoption of Explainable AI (XAI) with a focus on three properties: Quality of explanation, the explanation summaries should be consistent across multiple XAI methods; Architectural Compatibility, for effective integration in XAI, the architecture styles of both the XAI methods and the models to be explained must be compatible with the framework; Configurable operations, XAI explanations are operable, akin to machine learning operations. Thus, an explanation for AI models should be reproducible and tractable to be trustworthy. We present XAIport, a framework of XAI microservices encapsulated into Open APIs to deliver early explanations as observation for learning model quality assurance. XAIport enables configurable XAI operations along with machine learning development. We quantify the operational costs of incorporating XAI with three cloud computer vision services on Microsoft Azure Cognitive Services, Google Cloud Vertex AI, and Amazon Rekognition. Our findings show comparable operational costs between XAI and traditional machine learning, with XAIport significantly improving both cloud AI model performance and explanation stability.

link: http://dx.doi.org/10.1145/3639476.3639759

DISL: Fueling Research with A Large Dataset of Solidity Smart Contracts

Gabriele Morello, Mojtaba Eshghie, Sofia Bobadilla, Martin Monperrus

The DISL dataset features a collection of $514,506$ unique Solidity files that have been deployed to Ethereum mainnet. It caters to the need for a large and diverse dataset of real-world smart contracts. DISL serves as a resource for developing machine learning systems and for benchmarking software engineering tools designed for smart contracts. By aggregating every verified smart contract from Etherscan up to January 15, 2024, DISL surpasses existing datasets in size and recency.

link: http://arxiv.org/abs/2403.16861v2

INPC: Implicit Neural Point Clouds for Radiance Field Rendering

Florian Hahlbohm, Linus Franke, Moritz Kappel, Susana Castillo, Marc Stamminger, Marcus Magnor

We introduce a new approach for reconstruction and novel-view synthesis of unbounded real-world scenes. In contrast to previous methods using either volumetric fields, grid-based models, or discrete point cloud proxies, we propose a hybrid scene representation, which implicitly encodes a point cloud in a continuous octree-based probability field and a multi-resolution hash grid. In doing so, we combine the benefits of both worlds by retaining favorable behavior during optimization: Our novel implicit point cloud representation and differentiable bilinear rasterizer enable fast rendering while preserving fine geometric detail without depending on initial priors like structure-from-motion point clouds. Our method achieves state-of-the-art image quality on several common benchmark datasets. Furthermore, we achieve fast inference at interactive frame rates, and can extract explicit point clouds to further enhance performance.

link: http://arxiv.org/abs/2403.16862v1

SIP: Autotuning GPU Native Schedules via Stochastic Instruction Perturbation

Guoliang He, Eiko Yoneki

Large language models (LLMs) have become a significant workload since their appearance. However, they are also computationally expensive as they have billions of parameters and are trained with massive amounts of data. Thus, recent works have developed dedicated CUDA kernels for LLM training and inference instead of relying on compilergenerated ones, so that hardware resources are as fully utilized as possible. In this work, we explore the possibility of GPU native instruction optimization to further push the CUDA kernels to extreme performance. Contrary to prior works, we adopt an automatic optimization approach by defining a search space of possible GPU native instruction schedules, and then we apply stochastic search to perform optimization. Experiments show that SIP can further improve CUDA kernel throughput by automatically discovering better GPU native instruction schedules and the optimized schedules are tested by 10 million test samples.

link: http://arxiv.org/abs/2403.16863v1

Encoding of lexical tone in self-supervised models of spoken language

Gaofei Shen, Michaela Watkins, Afra Alishahi, Arianna Bisazza, Grzegorz Chrupa■a

Interpretability research has shown that self-supervised Spoken Language Models (SLMs) encode a wide variety of features in human speech from the acoustic, phonetic, phonological, syntactic and semantic levels, to speaker characteristics. The bulk of prior research on representations of phonology has focused on segmental features such as phonemes; the encoding of suprasegmental phonology (such as tone and stress patterns) in SLMs is not yet well understood. Tone is a suprasegmental feature that is present in more than half of the world's languages. This paper aims to analyze the tone encoding capabilities of SLMs, using Mandarin and Vietnamese as case studies. We show that SLMs encode lexical tone to a significant degree even when they are trained on data from non-tonal languages. We further find that SLMs behave similarly to native and non-native human participants in tone and consonant perception studies, but they do not follow the same developmental trajectory.

link: http://arxiv.org/abs/2403.16865v1

Lessons Learned from Building Edge Software System Testbeds

Tobias Pfandzelter, David Bermbach

Edge computing requires the complex software interaction of geo-distributed, heterogeneous components. The growing research and industry interest in edge computing software systems has necessitated exploring ways of testing and evaluating edge software at scale without relying on physical infrastructure. Beyond simulation, virtual testbeds that emulate edge infrastructure can

provide a cost-efficient yet realistic environment to evaluate edge software. In this experience paper, we share lessons learned from building a total of five edge software testbeds. We describe pitfalls in architecture and development as well as experiences from having students use our testbed tooling in distributed systems prototyping classes. While we remain confident that building custom testbed tooling is the right approach for edge computing researchers and practitioners alike, we hope this paper allows others to avoid common mistakes and benefit from our experience.

link: http://arxiv.org/abs/2403.16869v1

Conformal Off-Policy Prediction for Multi-Agent Systems

Tom Kuipers, Renukanandan Tumu, Shuo Yang, Milad Kazemi, Rahul Mangharam, Nicola Paoletti

Off-Policy Prediction (OPP), i.e., predicting the outcomes of a target policy using only data collected under a nominal (behavioural) policy, is a paramount problem in data-driven analysis of safety-critical systems where the deployment of a new policy may be unsafe. To achieve dependable off-policy predictions, recent work on Conformal Off-Policy Prediction (COPP) leverage the conformal prediction framework to derive prediction regions with probabilistic guarantees under the target process. Existing COPP methods can account for the distribution shifts induced by policy switching, but are limited to single-agent systems and scalar outcomes (e.g., rewards). In this work, we introduce MA-COPP, the first conformal prediction method to solve OPP problems involving multi-agent systems, deriving joint prediction regions for all agents' trajectories when one or more "ego" agents change their policies. Unlike the single-agent scenario, this setting introduces higher complexity as the distribution shifts affect predictions for all agents, not just the ego agents, and the prediction task involves full multi-dimensional trajectories, not just reward values. A key contribution of MA-COPP is to avoid enumeration or exhaustive search of the output space of agent trajectories, which is instead required by existing COPP methods to construct the prediction region. We achieve this by showing that an over-approximation of the true JPR can be constructed, without enumeration, from the maximum density ratio of the JPR trajectories. We evaluate the effectiveness of MA-COPP in multi-agent systems from the PettingZoo library and the F1TENTH autonomous racing environment, achieving nominal coverage in higher dimensions and various shift settings.

link: http://arxiv.org/abs/2403.16871v1

Proprioception Is All You Need: Terrain Classification for Boreal Forests

Damien LaRocque, William Guimont-Martin, David-Alexandre Duclos, Philippe Giguère, François Pomerleau

Recent works in field robotics highlighted the importance of resiliency against different types of terrains. Boreal forests, in particular, are home to many mobility-impeding terrains that should be considered for off-road autonomous navigation. Also, being one of the largest land biomes on Earth, boreal forests are an area where autonomous vehicles are expected to become increasingly common. In this paper, we address this issue by introducing BorealTC, a publicly available dataset for proprioceptive-based terrain classification (TC). Recorded with a Husky A200, our dataset contains 116 min of Inertial Measurement Unit (IMU), motor current, and wheel odometry data, focusing on typical boreal forest terrains, notably snow, ice, and silty loam. Combining our dataset with another dataset from the state-of-the-art, we evaluate both a Convolutional Neural Network (CNN) and the novel state space model (SSM)-based Mamba architecture on a TC task. Interestingly, we show that while CNN outperforms Mamba on each separate dataset, Mamba achieves greater accuracy when trained on a combination of both. In addition, we demonstrate that Mamba's learning capacity is greater than a CNN for increasing amounts of data. We show that the combination of two TC datasets yields a latent space that can be interpreted with the properties of the terrains. We also discuss the implications of merging datasets on classification. Our source code and dataset are publicly available online: https://github.com/norlab-ulaval/BorealTC.

link: http://arxiv.org/abs/2403.16877v1