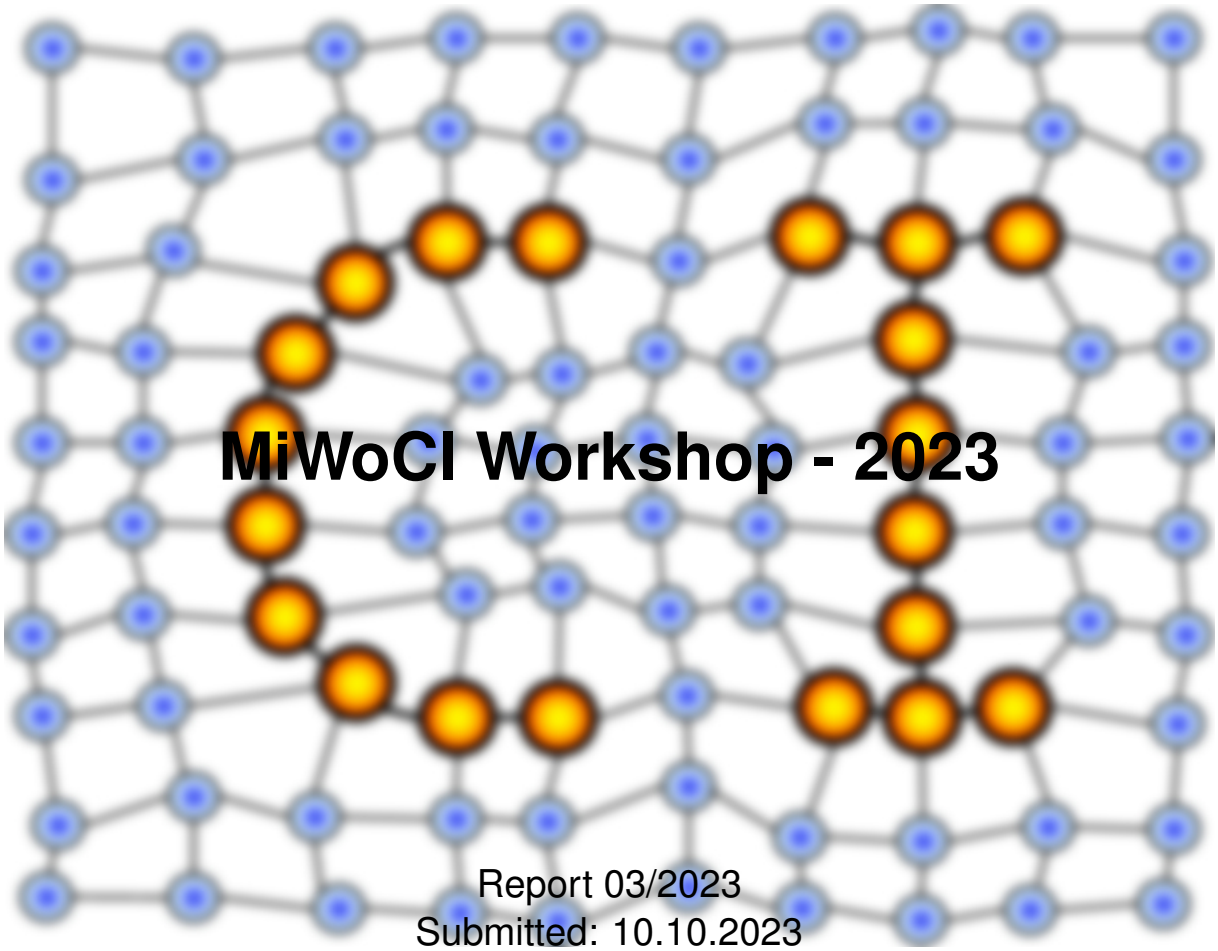
MACHINE LEARNING REPORTS



MiWoCI Workshop - 2023

Report 03/2023
Submitted: 10.10.2023
Published: 23.10.2023

Frank-Michael Schleif[1,2*,3*], Sven Hellbach[4], Marika Kaden[2], Thomas Villmann[2] (Eds.)
(1) Technical University of Applied Sciences Wuerzburg-Schweinfurt,
Sanderheinrichsleitenweg 20, 97074 Wuerzburg, Germany (2) University of Applied Sciences
Mittweida, Technikumplatz 17, 09648 Mittweida, Germany (3) University of Birmingham,
School of Computer Science,
Edgbaston, B15 2TT Birmingham, UK
(4) University of Applied Sciences Zwickau, Kornmarkt 1, 08012 Zwickau, Germany

Impressum

Publisher:	University of Applied Sciences Mittweida Technikumplatz 17, 09648 Mittweida, Germany
Editor:	Prof. Dr. Thomas Villmann Prof. Dr. Frank-Michael Schleif
Technical-Editor:	Prof. Dr. Frank-Michael Schleif
Contact:	frank-michael.schleif@fhws.de
URL:	http://techfak.uni-bielefeld.de/∼ fschleif/mlr/mlr.html
ISSN:	1865-3960

Abstracts of the 15^{th} Mittweida Workshop on Computational Intelligence - MiWoCI 2023 -

Frank-Michael Schleif, Sven Hellbach, Marika Kaden, and Thomas Villmann

Machine Learning Report 03/2023

Preface

The 15 th international *Mittweida Workshop on Computational Intelligence* (MiWoCI) gathering together more than 40 scientists from different universities including Bielefeld, Groningen, UAS Mittweida, UAS Würzburg-Schweinfurt, UAS Zwickau, Dr. Ing. h.c. F. Porsche AG in Weissach and NEC Laboratories Europe, Heidelberg. This year we could again gathering together in Mittweida, Germany. For all who could not attend in person the workshop was hybrid. Thus, from 23.8 - 25.8.2023 the tradition of scientific presentations, vivid discussions, and exchange of novel ideas at the cutting edge of research was continued. They were connected to diverse topics in computer science, automotive industry, and machine learning.

This report is a collection of abstracts and short contributions about the given presentations and discussions, which cover theoretical aspects, applications, as well as strategic developments in the fields.

Contents

Evaluation of interpretability - an ill-posed question?

Dietlind Zühlke

Technische Hochschule Köln

Abstract

When we as developers of machine learning (ML) approaches and ML applications are talking about evaluating of ML, we often mean to measure as precise and general as possible certain characteristics of the model or approach concerned. However, interpretability - which is much more of a cognitive dimension, different for every individual human - is no mathematical concept or characteristics and thus we lack formal approaches to it from our domain. However evaluating such cognitive and social dimensions has been done successfully for years in the cognitive and social sciences, from where we get inspiration on the characteristics and dimensions that need to be taken into account. It is important to be very precise about the users of the interpretability means as well as their specific interpretability needs [1]. And still some areas like allowing the interpretable assessment of data used in modeling, are neither considered by classical interpretability nor their evaluation. When taking into account all details of evaluation it seems impossible to come to a rigorously valid and precise evaluation. Thus we need to come up with pragmatical but reflected iterative evaluation approaches together with all stakeholders all over the development of approaches and applications.

References

[1] Escalante, H. J., Escalera, S., Guyon, I., Baró, X., Güçlütürk, Y., Güçlü, U., & van Lier, R. (Eds.). (2018). Explainable and interpretable models in computer vision and machine learning. Cham, Switzerland: Springer International Publishing.

A framework for model informed posterior construction

Elisa Oostwal

Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, The Netherlands

Abstract

Time-series is an important type of input data for classification procedures. The available data may be limited in terms of quantity and quality, which results in poor results when using traditional statistical machine learning techniques. To resolve these limitations, domain knowledge can be incorporated by, for example, introducing a mechanistic model. The Learning in the Model Space framework then proposes to represent every time-series by a parametrization of the given model, which can be found using parameter estimation techniques, and perform classification using this representation. Partially observed dynamical systems often present an issue, since multiple parameter combinations can produce identical observable dynamic output. This makes it impossible to uniquely determine which parameter configuration best explains a given time-series observation. To capture the uncertainty in the parameter estimates due to the variability of observations as well as unidentifiabilities inherent to the system, a Bayesian approach is proposed. A *posterior* is constructed for every time-series data, quantifying the level of belief for every possible parametrization of the given mechanistic system. The posterior is typically not analytically tractable, but can be approximated using sampling algorithms.
We present a framework for informed posterior construction for partially observed dynamical systems, that can be used in the context of the *Learning in the Model Space* framework. We prove that a compact representation of the distribution that eliminates redundant information exists, allowing for more efficient sampling.

About Interpretability of Prototype Models

Ronny Schubert

Saxon Institute of Computational Intelligence and Machine Learning (SICIM),
Hochschule Mittweida, Germany

September 27, 2023

Abstract

When it comes to *human-machine interaction* in artificial intelligence and machine learning *Explainability* and *Interpretability* are important and highly discussed present-day terms, not only within the respective research communitites, but also in politics [1]. White-box models are often considered *ante-hoc* interpretable. However, even *ante-hoc* models come with a small print, which states, that *explainees* need a certain understanding and knowledge to comprehend the respective models, thus making the effect of interpretability audience dependent and not well-defined [2]. Consequently, we want to explore and discuss the impact of such critique in the frame of prototype models, i.e. future model development and explanation methods, as well as already existing approaches, since these models are often termed *ante-hoc* interpretable.

References

[1] European Commission. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206, 2021.

[2] Sokol, Kacper and Vogt, Julia E. (Un)reasonable Allure of Ante-hoc Interpretability for High-stakes Domains: Transparency Is Necessary but Insufficient for Comprehensibility. 10.48550/ARXIV.2306.02312. 2023.

Testing Stationarity – Why Drift Detection for Time Series is Boring

Fabian Hinder and Barbara Hammer

Bielefeld University, Germany

Abstract

A common assumption in time series analysis is stationary, that is the distribution of the process X_t is the same for all time points, i.e., $F_{X_t} = F_{X_{t'}}$ for all t, t'. Therefore, relevant problems are given by testing for whether or not a given time series is stationary or determining the change points if not. These problems are closely related to drift detection in the context of data streams. From a theoretical point of view, the main difference between both setups is that in data streams the observations are usually assumed to be independent while in time series the observations of consecutive time points depend on each other, e.g., a common assumption is that the series is continuous. Thus, fundamental statistical results like the law of large numbers or the central limit theorem no longer hold true. Also, the rate of convergence of several estimators is significantly changed. Hence, common testing mechanisms can no longer be applied.

In this talk, we discuss the implications of dependency of data points for the question of testing for stationary and concept drift. In particular, we address the question of whether there do exist instantiations of this setup that are non-trivial and admit a non-trivial test.

Learning Intrinsic Properties of Riemannian Manifolds

Andreas Mazur, Fabian Hinder and Barbara Hammer

Bielefeld University, Germany

Abstract

Convolutional Neural Networks (CNNs) have led to astonishing performances in many different applications such as computer vision, natural language processing and more [2]. However, standard CNNs lack the ability of processing non-Euclidean data such as graphs and manifolds. While the success of Graph Neural Networks (GNNs) got a lot of attention [4], the advancements in processing manifolds, such as object surfaces, got comparably little. This elaboration is devoted to raise attention on the problem domain of learning intrinsic properties of manifolds with Intrinsic Mesh CNNs (IMCNNs) [1] and initiate a discussion about possible improvements. We do so by providing a short overview on how IMCNNs work, especially focusing on the patch-operator, and describe typical problem domains in which they achieve remarkable performances. Furthermore, we counteract the lack of available implementations by providing an alpha version of our IMCNN-library *GeoConv* [3], thereby allowing the user to easily try out new ideas. We finish our talk with a discussion about so far unused weight functions within the patch-operator.

References

[1] Michael M. Bronstein et al. *Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges*. 2021. DOI: 10.48550/ARXIV.2104.13478. URL: https://arxiv.org/abs/2104.13478.

[2] Zewen Li et al. "A survey of convolutional neural networks: analysis, applications, and prospects". In: *IEEE transactions on neural networks and learning systems* (2021).

[3] Andreas Mazur. *GeoConv - Geodesic Convolutions with Tensorflow*. URL: https://github.com/andreasMazur/geoconv.

[4] Zonghan Wu et al. "A Comprehensive Survey on Graph Neural Networks". In: *IEEE Transactions on Neural Networks and Learning Systems* 32.1 (2021), pp. 4–24. DOI: 10.1109/TNNLS.2020.2978386.

Enabling Cost-Efficient Ownership of Connectionist AI-Models on a Decentralized Blockchain Database.

Shilpa Babu and Frank Ortmeier

Otto von Guericke University Magdeburg, Magdeburg, Germany

Andreas Backhaus and Udo Seiffert

Compolytics GmbH, Barleben, Germany

August 11, 2023

Abstract

Artificial Neural Networks are vital for modern sensor systems, requiring substantial resources and protection by manufacturers. On the other side, customers seek permissionless ownership of digital artefacts, while ensuring model integrity and regulatory compliance. This study proposes leveraging blockchain platforms to balance manufacturer and customer interests. Representing model ownership as non-fungible tokens (NFTs) establishes true digital ownership. However, storing complete neural networks on platforms like Ethereum is impractical. To address this, we present a novel method utilizing connectionist information storage in neural networks.

By employing standard pruning mechanisms, we extract parameters from the network that have the greatest impact on model performance. These parameters are then stored directly in the NFT contract on the blockchain, while the residual model is stored on an open webspace like IPFS. This approach ensures that unauthorized participants cannot utilize the stored model. To assess the effectiveness of our method, we conduct a qualitative assessment using various neural network methods and perform a quantitative cost evaluation to determine the trade-off between on-chain storage costs and the resulting performance degradation.

In conclusion, our study proposes a method for storing neural networks on the blockchain, enabling permissionless ownership of digital artefacts while safeguarding the interests of both manufacturers and customers. By leveraging the connectionist information storage within neural networks and combining it with blockchain technology, we establish a framework that provides transparency, security, and accountability in the ownership and usage of AI models. Through a comprehensive assessment, we determine the optimal balance between storage costs and performance degradation, facilitating informed decision-making for stakeholders in the domain of AI model ownership.

Iterated Relevance Matrix Analysis: IRMA to the rescue

Sofie Lövdal[1,2] and Michael Biehl[1]

[1] Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, Univ. of Groningen, Nijenborgh 9, 9747 AG Groningen - The Netherlands

[2] University Medical Center Groningen (UMCG), Dept. of Nuclear Medicine and Molecular Imaging, Hanzeplein 1, 9713 GZ Groningen -The Netherlands

Abstract

In the first part of the presentation, we introduce the Iterated Relevance Matrix Analysis (IRMA) [1] for the improved interpretation of feature relevances in classification problems. The suggested method identifies a linear subspace of features representing the classification specific information in the considered data sets. By iteratively determining a new discriminative direction while projecting out all previously identified ones, all features carrying relevant information about the target classification can be found. This facilitates a detailed analysis of the feature relevances and improved discriminative visualizations of the data.

Next we illustrate the use of IRMA for the correction of biases in data sets which originate from different sources. As an example we consider the classification of FDG-PET brain scans for the diagnosis of neurodegenerative diseases [2]. In a first phase, the subspace S related to the discrimination of sources, i.e. medical centers, is identified by applying IRMA in a multi-center cohort of healthy control subjects. In the second phase, a GMLVQ classifier is trained with respect to the target diseases in the remaining subspace orthogonal to S.

References

[1] S. Lövdahl, M. Biehl: Improved Interpretation of Feature Relevances: Iterated Relevance Matrix Analysis (IRMA). ESANN 2023, accepted contribution.

[2] R. van Veen, N.R. Bari Tambolia, S. Lövdal et al.: Subspace Corrected Relevance Learning with Application in Neuroimaging. Submitted, 2023.

Switching Roles – Which technical tools do you need to do your research?

Johannes Brinkrolf

Bielefeld University, CITEC, Germany

Abstract

For research, the amount of data that has to be processed is increasing rapidly, and larger computing capacities are needed [1]. Especially for training, fine-tuning, or working with deep neural networks, the technical requirements are enormous and are typically not satisfied by the hardware of a single workstation. Thus, servers for high-performance computing (HPC) are required. They usually contain a network of PCs with multiple GPUs. Computational tasks from several users can then be scheduled on this cluster using a management system, e.g. SLURM [2]. In addition to the GPU resources, fast and large storage is needed to enable state-of-the-art research.

In this talk, I want to recap the change in the requirements for services of computing power. Further, I show what is essential for providing a GPU cluster and demonstrate the technical view for operating such one. In the end, I discuss what requirements might be asked for in the next five years.

References

[1] Petroc Taylor. "Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025". URL: `https://www.statista.com/statistics/871513/worldwide-data-created/`. [Online; accessed 13th July, 2023]. 2022.

[2] Andy B. Yoo, Morris A. Jette, and Mark Grondona. "SLURM: Simple Linux Utility for Resource Management". In: *Job Scheduling Strategies for Parallel Processing, 9th International Workshop, JSSPP 2003, Seattle, WA, USA, June 24, 2003*. Ed. by Dror G. Feitelson, Larry Rudolph, and Uwe Schwiegelshohn. Vol. 2862. Lecture Notes in Computer Science. Springer, 2003, pp. 44-60. DOI: 10.1007/10968987_3. URL: `https://doi.org/10.1007/10968987_3`.

Large language models and the future of computer programming

Benjamin Paaßen

Bielefeld University

Abstract

Looking at the performance of large language models, programming may seem like an outdated skill. In the future, we may simply feed a natural language problem description into a model such as Github Copilot or AlphaCode and get out a computer program that solves our problem [1, 3] — or can we? Recent work provides evidence that generated programs may sometimes be dysfunctional, fail to respect constraints mentioned in the prompt, or include security vulnerabilities and bugs [2, 5, 4, 7]. We explain these failures by a lack of *computational thinking*, meaning the capacity for decomposition, abstraction, algorithms, debugging, iteration, and generalization [6]. Accordingly, highly skilled human workers are still required to translate real-world problems into input for code generation, guide the code generation process, and verify the generated programs. As tools for such a collaborative code generation process, we will also require new machine learning models, which are more interactive, iterative, and interpretable.

References

[1] Chen et al. (2021). Evaluating Large Language Models Trained on Code. https://arxiv.org/abs/2107.03374

[2] Dakhel et al. (2022). GitHub Copilot AI pair programmer: Asset or Liability? https://arxiv.org/abs/2206.15331

[3] Li et al. (2022). Competition-level code generation with AlphaCode. https://doi.org/10.1126/science.abq1158

[4] Pearce et al. (2022). Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions. Proceedings of the SP, 754-768. https://doi.org/10.1109/SP46214.2022.9833571

[5] Perry et al. (2022). Do Users Write More Insecure Code with AI Assistants? https://arxiv.org/abs/2211.03622

[6] Shute et al. (2017). Demystifying computational thinking. Educational Research Review, 22, 142-158. https://doi.org/10.1016/j.edurev.2017.09.003

[7] Sobania et al. (2023). An Analysis of the Automatic Bug Fixing Performance of ChatGPT. https://arxiv.org/abs/2301.08653

Symmetric Structural Autoencoder for Images applied on from Microgravity Experiments

Daniel Staps and Marika Kaden

SICIM, Univ. of Appl. Sciences Mittweida, Germany

Abstract

During experiments under microgravity, e.g. on the ISS, a lot of data often accumulates quickly, and memory, computing capacity and transmission speed are limited. In the lecture, we present the so-called symmetric structural autoencoder (SyS-AE) for image reconstruction. This model is very sparse and memory efficient due to its symmetric structure. Furthermore, it aims to preserve the perceptual properties in the decoded images for later visual inspection by experts. In the presentation we show the exact structure of the Sys-AE and show first results.

Acknowledgment

This work was funded by the German Aerospace Research Center (projects AIMS/DAIMLER grant: 50WK2270A and AIMS/IAI-XPRESS grant: 50WK2270)

Equilibrium analysis of multilayer feedforward neural networks

Otavio Citton

Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, Univ. of Groningen, Nijenborgh 9, 9747 AG Groningen - The Netherlands

Abstract

In this presentation, we extend the analysis of Soft Committee Machines in a student-teacher scenario using the framework of statistical mechanics. Specifically, we compare the effects of different activation function, namely the ReLU and the sigmoid, on the overall behavior of the network. We investigate the equilibrium state of the network using the replica method, in particular the low temperature regime and its effects on the generalization and training error, as well as its entropy. We also hint on how to build upon this approach to study sparsity in these networks.

A Primer on Over-Squashing and Over-Smoothing Phenomena in Graph Neural Networks

Simon Heilig

Master Data Science
Friedrich-Alexander University of Erlangen-Nuremberg
simon.heilig@fau.de

Abstract

In the last years, graph neural networks (GNN) have gained a lot of attraction in research. Thanks to their ability to embed graph structures, numerous downstream tasks can now be successfully addressed at the level of nodes, edges, and graphs. Despite their success, increasing the number of layers to capture long-term dependencies leads to over-squashing and over-smoothing of feature representations. After gaining intuition about why and where the problems occur, this talk focuses on strategies to overcome over-squashing. Inspired by the formulation of deep neural architectures as stable and non-dissaptive ODEs, long-term dependencies in the information flow can be preserved. Finally, an outlook on a different formulation in terms of Hamiltonian dynamics is given.

Design of an Attention Integration into Learning Vector Quantization

Thomas Davies

Saxon Institute of Computational Intelligence and Machine Learning (SICIM),Hochschule Mittweida, Germany

August 24, 2023

Abstract

Machine learning models for timeseries have always been a special topic of interest due to their unique data structure. Recently, the introduction of attention improved the capabilities of recurrent neural networks and transformers with respect to their learning tasks such as machine translation [1–3]. However, these models are usually subsymbolic architectures, making their inner working hard to interpret without comprehensive tools. In contrast, interpretable models such learning vector quantization are more transparent in the ability to interpret their decision process [4]. This talk briefly presents the attempt to merge attention as a machine learning function with learning vector quantization to better handle timeseries data. The experiments for the proposed design will briefly be presented. Although the proposed model did not yield the expected results, the talk outlines improvements for further research on this approach.

References

[1] A. Vaswani *et al.*, "Attention is all you need," *CoRR*, vol. abs/1706.03762, 2017. arXiv: 1706.03762. [Online]. Available: http://arxiv.org/abs/1706.03762.

[2] K. Cho, A. Courville, and Y. Bengio, "Describing multimedia content using attention-based encoder-decoder networks," *IEEE Transactions on Multimedia*, vol. 17, no. 11, pp. 1875–1886, 2015. DOI: 10.1109/TMM.2015.2477044.

[3] S. Chaudhari, G. Polatkan, R. Ramanath, and V. Mithal, "An attentive survey of attention models," *CoRR*, vol. abs/1904.02874, 2019. arXiv: 1904.02874. [Online]. Available: http://arxiv.org/abs/1904.02874.

[4] D. Nova and P. Estevez, "A review of learning vector quantization classifiers," *Neural Computing and Applications*, vol. 25, Sep. 2014. DOI: 10.1007/s00521-013-1535-3.

Test Group Study: Driver Interventions during Assisted Driving

Robin Schwager

Dr. Ing. h.c. F. Porsche AG, Weissach, Germany

Abstract

When using automated driving functions, humans continuously provide feedback by interacting with the vehicle and intervening if they are unsatisfied with the function's behavior. This feedback is currently unused but could be utilized to adapt the function's behavior to the driver's individual wishes. Such human machine cooperation can be used to further increase human acceptance of driver assistance systems and automated driving functions. To analyze these corrections by the drivers, a test group study was conducted where each test subject used a test vehicle for one week and recorded their daily commuting route. During the drives, a predictive longitudinal driving function was used and all needed corrections by the drivers were annotated using voice annotations. In these voice annotations, the drivers explain why they intervened in the given situation. The test subjects were explicitly told not only to intervene when they must (e.g., due to traffic situations the driving function was not intended for), but also especially intervene when they are unsatisfied with the function?s behavior. For example, if the function drives too slowly through a specific curve, the driver intervenes with the gas pedal, accelerating the vehicle to their desired speed. After their test drives, each participant filled out a questionnaire, inquiring about their satisfaction with the system and how they felt about the number of needed corrections. From this study, a dataset was created, consisting of all vehicle bus signals during the drives (time series data), the voice annotations of each intervention, and the questionnaire. This presentation will cover the basics of driver interventions within and outside the system boundaries, highlight the current status of the dataset and planned/ongoing analyses, as well as explore some exemplary data to showcase the dataset.

Unsupervised clustering of steroid metabolome profiles in women with PCOS

Roland J. Veen[1],
Eka Melson, Thais P. Rocha, Lida Abdi, Tara McDonnell, Veronika Tandl, James M. Hawley, Laura B.L. Wittemans, Amarah V. Anthony, Lorna C. Gilligan, Fozia Shaheen, Punith Kempegowda, Caroline D.T. Gillett, Leanne Cussen, Cornelia Missbrenner, Fannie Lajeunesse-Trempe, Helena Gleeson, Aled Rees, Lynne Robinson, Channa Jayasena, Harpal S. Randeva, Georgios K. Dimitriadis, Larissa G. Gomes, Alice J. Sitch, Eleni Vradi, Barbara Obermayer-Pietsch, Michael W. OâReilly, Angela E. Taylor, Michael Biehl[1], Wiebke Arlt

[1]Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, The Netherlands
Additional Authors from: Sao Paulo, Brazil - Birmingham / Manchester / Oxford / Cardiff / London / Coventry, United Kingdom - Dublin, Ireland - Graz, Austria - Berlin, Germany

Introduction: Polycystic ovary syndrome (PCOS) affects 10% of women and is associated with a two- to threefold risk of type 2 diabetes, hypertension, fatty liver, and cardiovascular disease. Androgen excess has been implicated as a major contributor to metabolic risk in PCOS. We aimed to identify PCOS subtypes with distinct androgen profiles and to compare their cardiometabolic risk.

Methods: We cross-sectionally studied 488 treatment-naive women with PCOS from UK & Ireland, Austria and Brazil (Age 28[24-32] years; BMI 27.5[22.4-34.6] kg/m2). We quantified 11-androgenic serum steroids by tandem mass spectrometry, followed by unsupervised k-means clustering of Z-score transformed steroid data and statistical comparison of differences in clinical phenotype and metabolic parameters.

Results: Machine learning identified three distinct subgroups of PCOS characterised by gonadal-derived androgen excess (GAE), adrenal-derived androgen excess (AAE), and comparably mild androgen excess (MAE), with similar age and BMI. Using cross-validation and applying Generalised Matrix Learning Vector Quantisation on the found clusters, we validated the robustness of our clustering solution.

Conclusion: Unsupervised cluster analysis revealed three PCOS subtypes with distinct androgen excess profiles. The AAE cluster was characterised by the highest insulin resistance, impaired glucose tolerance, and type 2 diabetes, implicating 11-oxygenated (adrenal-derived) androgens as drivers of metabolic risk. These results provide proof-of-principle for a novel metabolic risk prediction tool in PCOS that could guide future preventive and therapeutic strategies.

Comparison of Autoscaling Frameworks for Containerized Machine-Learning-Applications in a Local and Cloud Environment

Christian Schröder[1] , René Böhm[1] , and Alexander Lampe[2]

[1] Vitesco Technologies GmbH, Limbach-Oberfrohna, Germany christian.2.schroeder@vitesco.com, rene.boehm@vitesco.com

[2] Dept. Engineering, University of Applied Sciences, Mittweida Germany lampe@hs-mittweida.de

Abstract

When it comes to deploying machine learning applications, the automated allocation of computing resources (Autoscaling) is crucial for delivering a constant inference time under fluctuating workloads. The aim is to maximize the Quality of Service requirements of performance and scalability while minimizing the resource costs. In this paper, we present a comparison of scalable deployment methods on three scaling levels: application level (TorchServe, RayServe), on container level in a local environment (K3s) and on container and machine level in a cloud environment (Amazon Web Services Elastic Container Service and Elastic Kubernetes Service). Comparison is done by investigation of average and standard deviation of inference time in a multi client scenario as well as upscaling response times. As a result, a local and cloud-based deployment strategy is proposed.

Keywords Autoscaling, Kubernetes, Amazon Web Services, RayServe, TorchServe

Localizing small leakages by means of drift explanations

Valerie Vaquet, Fabian Hinder, Barbara Hammer

Bielefeld University, Germany

Abstract

Facing climate change, the already limited availability of drinking water will decrease in the future rendering drinking water an increasingly scarce resource [1]. Considerable amounts of water are lost through leakages in water transportation and distribution networks. Leakage detection and localization are challenging problems due to the complex interactions and changing demands in water distribution networks. Especially small leakages are hard to pinpoint, yet their localization is vital to avoid water loss over long periods of time. While there exist different approaches to solving the tasks of leakage detection and localization, they are relying on various information about the system, e.g. real-time demand measurements and the precise network topology, which is an unrealistic assumption in many real-world scenarios [2].

In contrast, in this work, we attempt leakage localization using pressure measurements only. For this purpose, we first model leakages in the water distribution network using Bayesian networks and analyze the system dynamics. We then show how the problem is connected to and can be considered through the lens of concept drift. In particular, we argue that model-based explanations of concept drift [3] are a promising tool for localizing leakages given limited information about the network. The methodology is experimentally evaluated using realistic benchmark scenarios.

References

[1] Rodell, Matthew and Famiglietti, Jay S and Wiese, David N and Reager, JT and Beaudoing, Hiroko K and Landerer, Felix W and Lo, M-H. "Emerging trends in global freshwater availability". In: *Nature* 7707 (2018), 651–659. URL: https://doi.org/10.1038/s41586-018-0123-1.

[2] Hu, Zukang and Chen, Beiqing and Chen, Wenlong and Tan, Debao and Shen, Dingtao. "Review of model-based and data-driven approaches for leak detection and location in water distribution systems". In: *Water Supply* 7 (2021), pp. 3282–3306. URL: https://doi.org/10.2166/ws.2021.101.

[3] Hinder, Fabian and Artelt, André and Vaquet, Valerie and Hammer, Barbara. "Contrasting Explanation of Concept Drift". In: *ESANN 2022 proceedings*(2022), pp. 293–298. URL: https://www.esann.org/sites/default/files/proceedings/2022/ES2022-71.pdf.

Forecast of market potentials for a tool manufacturer

Lukas Bader

UAS Köln/Bonn, Germany

Abstract

he work presented here is part of a research project that deals with the identification of market potentials for an industrial partner. A crucial component for the global strategy alignment is the determination of market potentials for different product groups in focus markets.
Determining the potential for specific markets is very complex and currently often based on purchased market studies of external providers. These studies are often non-transparent, as the exact methods and data sources are not clear. In a literature research it became clear that available literature in this area is often very product-specific and difficult to transfer to the tooling industry.
A first approach to solve this problem is to use a bottom-up method in combination with economic geographic data. The field of geographic economics deals, among other topics, with economic developments and interactions of geographic locations in a market. One consideration is to aggregate the individual potentials and developments of individual regions in a market using spatial data and thus to determine the overall potential of a product group for the market. In addition, a kind of industrial map of the market is created, which shows the development, especially with regard to emerging industrial centers. Through this analysis, it is possible to identify potential growth areas and generate recommendations for strategic decisions.

Keywords: Market potential, geographic economic data, bottom-up method

Adversarial Attacks on Leakage Detectors in Water Distribution Networks

Paul Stahlhofen

Bielefeld University, Germany

13th of July, 2023

Abstract

Adversarial attacks [3] pose problems to many state of the art Machine Learning models. These attacks, created by specifically crafted inputs that cause a model to make mistakes, require further investigation. Knowledge of adversarial weaknesses can be used to enhance model robustness, which is a key requirement of trustworthy AI [1]. Of particular importance is the robustness against adversarials for models which are applied in safety critical domains, such as the monitoring of water distribution networks (WDNs). Overviews on methodologies for the detection of leaks in WDNs can be found in [2].

This talk is concerned with finding weak spots of ML-driven leakage detection models. We focus on the search for the least sensitive point (LSP) of the detector, that is, the network node where the largest possible undetected leak could occur. After providing the methodologies used to find the least sensitive point we show results on two benchmark water distribution networks. The goal of upcoming research is to use knowledge about the LSP to enhance adversarial robustness of leakage detectors. Computational demand of the current search algorithm and a good strategy for robust incremental sensor placement are challenges that we would like to discuss.

References

[1] European Commission and Directorate-General for Communications Networks, Content and Technology: Ethics guidelines for trustworthy AI. Publications Office (2019). https://doi.org/doi/10.2759/346720

[2] Hu, Z., Chen, B., Chen, W., Tan, D., Shen, D.: Review of model-based and data-driven approaches for leak detection and location in water distribution systems. Water Supply **21**(7), 3282–3306 (04 2021). https://doi.org/10.2166/ws.2021.101, `https://doi.org/10.2166/ws.2021.101`

[3] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R.: Intriguing properties of neural networks. In: International Conference on Learning Representations (2014), `http://arxiv.org/abs/1312.6199`

Criticality-based treatment of radar points for parking applications

Tim Brühl

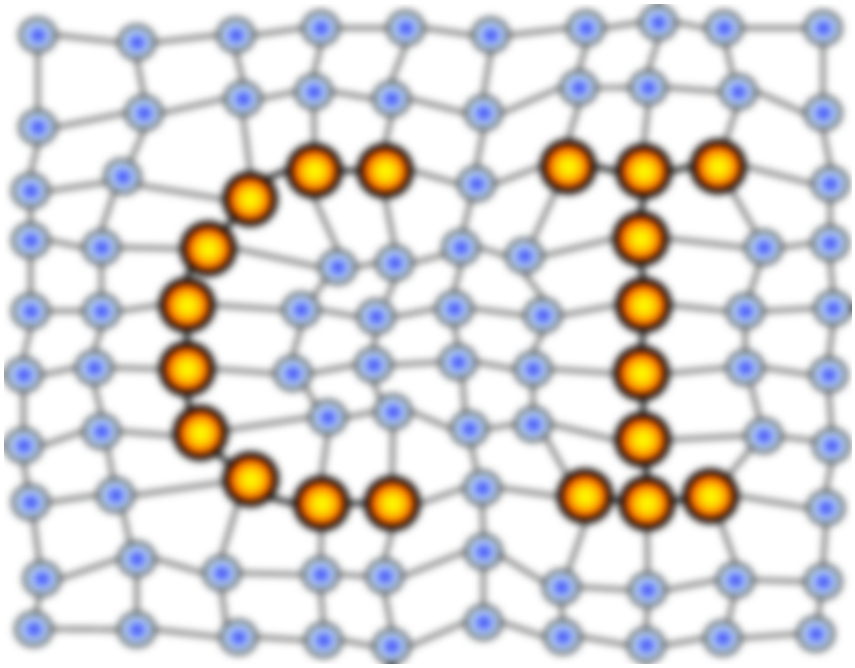
Dr. Ing. h.c. F. Porsche AG, D-71287 Weissach
Karlsruhe Institute of Technology, D-76131 Karlsruhe
tim.bruehl@porsche.de

Abstract

Radar sensors play a crucial role for highly automated driving and parking functions. Advantages are the robustness against weather impacts and the possibility to directly measure velocities. While in the past, the radar data was used mainly for object detection for functions like Adaptive Cruise Control and Lane Change Assistant, it gets increasingly interesting for other tasks such as free space detection or odometry estimation.
However, a radar point cloud is noisy due to effects like amplifier noise, interference, and clutter. Many points in the cloud do not match directly to an object but are False Positives. This means that it is a common approach to filter the point cloud in favor of keeping the False Alarm Rate low. During this, weak and unlikely targets are deleted. This procedure means that a certain rate of wrongly identified True Positive points are accepted, while the majority of deleted targets are False Positives. This approach is however not valid when it comes to developing safe functions for SAE level 4. In this level, the vehicle can maneuver autonomously without a driver inside, managing situations in a predefined domain on its own. Here, the driver cannot be engaged in uncertain situations, meaning that controllability is worse compared to level 2 functions. Thus, this level requires significantly lower failure in time rates.
In this talk, insight will be given on how this conflict can be solved. Filtering, i. e. deleting radar points, is only permissible if the respective radar point does not imply a potentially dangerous maneuver. The criticality of each point must be evaluated regarding aspects like controllability, exposure rate and severity of a hazardous situation induced by an erroneous delete of a True Positive point. Radar points without or with low criticality can be filtered as usual, whereas those with high criticality need to be treated specifically. Context of the radar points can be added by monitoring them in a temporal-spatial context, adding information of other radars in the belt or by taking camera information into account.
Applied to the function "Free Space Detection", this approach can guarantee free space to a very high rate, assuming that objects are indeed measured by the radar sensor. Future work will improve the radar information enhancement and adapt the idea to the radar odometry problem.

MACHINE LEARNING REPORTS

Report 03/2023



Impressum

Machine Learning Reports ISSN: 1865-3960

▽ Publisher/Editors

Prof. Dr. rer. nat. Thomas Villmann
University of Applied Sciences Mittweida
Technikumplatz 17, 09648 Mittweida, Germany
• http://www.mni.hs-mittweida.de/

Prof. Dr. rer. nat. Frank-Michael Schleif
Technical University of Applied Sciences Wuerzburg-Schweinfurt
Sanderheinrichsleitenweg 20, 97074 Wuerzburg, Germany
• https://fiw.thws.de/

▽ Acknowledgments

We would like to thank the reviewers for their time and patience.