Software Engineering Assignment

Emma Andersdotter Svensson, Umeå University

September 2024

1 Introduction

I work as a PhD student at the department of mathematics and mathematical statistics at Umeå university. My research is within the field of geometric deep learning, with the primary goal of increasing the mathematical understanding of neural network models through the lens of differential geometry. Our latest work has been to combine our previous knowledge in mainly differential geometry with so-called neural ordinary differential equations (neural ODEs), which are a family of neural network models. A neural ODE is not made up of a discrete set of hidden layers. Instead, it is defined by an ODE, where the input data is the initial condition of the ODE and the outputs are its solution. The network is defined by the vector field describing how the solution of the ODE evolves continuously over time. In our work, we formulate equivariant neural ODEs using the theory of differential invariants, among other things. We also prove that equivariant neural ODEs are universal approximators of any diffeomorphism.

In this essay, I go over some concepts introduced during the lectures and compare them to my own work. I also analyze two articles found on the 2024 CAIN conference.

2 Robert's lectures

Robert's lectures gave an overview of software engineering and what it entails. My main takeaway from them was that software engineering is more than just coding, but includes a large set of players working together to create a final product. While my work, on the surface, does not appear to have any relevance to software engineering, this made me realize that my work can still be regarded as a building block in a larger framework. In the second lecture, Robert talked about quality assurance in testing in software engineering. My discussion will mainly focus on this.

Some motivators of quality assurance and testing include the costs and potential dangers if something goes wrong. My work can help minimize such instances, since a larger understanding of the models at hand makes it easier to understand why something could go wrong and how to combat this.

Testing is introduced as a systematic evaluation of a software system to evaluate its quality. This can be done using both manual and automated methods. Some main problems in testing include the size of the input and/or output as well as the complexity of the system behaviour. With explainable AI – which my work is contributing to – the complexity of such systems is easier to understand, since it provides more information on what to look for.

One technique mentioned in the lecture was black-box testing, which can be summarized as a testing method where an application's functionality is examined without examining internal structures. One possible problem is that if the testing shows that something is wrong, it can be hard to combat this without considering the internal structure. With more mathematical descriptions and understanding, the inner-workings of a "black box" can be better understood.

3 Guest lecture

In the guest lecture from Saab, Per mentioned that one of the top answers to the question "How do you foresee Software Engineering relevance changing with the increased integration of AI/ML in your operation?" was that nothing will change and that AI is overrated. I think one of the reasons for this answer could be that AI is a relatively new subject that is not yet fully understood. By creating a robust mathematical framework for AI models and creating better models, the potential for AI could be more evident and also more welcome in operations.

Another question was "How do you foresee Software Engineering relevance changing with the integration of AI/ML in your products?", where he mentioned that the aspects of the ATM systems will be automated aren't only driven by technological capabilities. One factor is the safety of the AI techniques. The relevance to my work does, again, relate to understanding. By increasing the understanding of AI and neural network models, the room for error decreases and therefore increases the safety of AI techniques.

4 Papers

4.1 Towards a Responsible AI Metrics Catalogue: A Collection of Metrics for AI Accountability

The first paper I read is called “Towards a Responsible AI Metrics Catalogue: A Collection of Metrics for AI Accountability” [1] and is an article within the subject of Responsible AI (RAI). The authors mention the shortcomings of the current RAI frameworks, especially for accountability. To ensure accountability in AI systems, the authors develop a comprehensive set of metrics. The core ideas include the development of a metrics catalogue for AI accountability with a process-centric approach, a tripartite categorization of metrics, and they lay the groundwork for a comprehensive RAI framework.

The development of a comprehensive metrics catalogue for AI accountability is formulated through a systematic multivocal literature review (MLR). The tripartite categorization of the metrics is designed to implement accountability measures in AI systems. It is a categorization divided into three main types, namely process, resource and product metrics. The process metrics set the basic procedural standards. The resource metrics cover the essential frameworks and tools. Product metrics represent the final output.

While the paper does not focus on the same research area as mine, I did notice a common goal, namely the enhancement of the reliability and robustness of AI systems. One of the mentioned challenges of GenAI models was ”the big black box as scapegoat”, which essentially refers to how the complexity of GenAI models can deflect accountability from human decision-makers. As a mathematician, my goal is to use analysis and proof to achieve a better understanding. Increasing the fundamental understanding of AI models can help demystifying them.

A future development of my research could help improving the robustness and generalization of models where there is an inherent symmetry in the data. An example of a future project could be to map the flow lines of winds on the Earth, helping with weather forecasting. By combining my work with the accountability metrics described in the article, the project would be more ethically responsible and scientifically sound.

I’ll finish this section by mentioning how my research could be adapted to enhance AI engineering in the context of the paper. For one, procedural integrity and transparency could be included into my framework by integrating the accountability metrics from the paper. This has the benefit of making the models more ethically accountable. While ethical concerns may not be an issue at the moment, since my project is strictly theoretical, its future use could be in for example image recognition, where ethical concerns are important. Another idea from the paper that could be incorporated into my framework is the enhancement of documentation and transparency. When writing code, for example, saving the data and being able to provide the source code when requested is important. This increases the trust in the models.

4.2 Identifying architectural design decisions for achieving green ML serving

The second paper I read is called ”Identifying architectural design decisions for achieving green ML serving” [2]. It is a paper within green AI, which aims to make AI systems more energy efficient to reduce environmental impact.

The authors highlight the importance of optimizing the inference phase in machine learning models, which is often overlooked in the context of energy consumption. This provides more insight into how AI systems can be made more cost-effective and sustainable. They identify architectural design decisions that could influence energy efficiency. They also give an overview of quality characteristics such as energy efficiency.

The most evident similarity between my work and the paper is the common goal of efficiency. This goal, however, is looked at from different angles. The way my work can contribute to the efficiency of AI models is by incorporating symmetries and invariance of the data into such models.

My research could fit into a larger AI-intensive software project by enhancing the efficiency of ML models with an underlying symmetry. By creating models that have the underlying symmetries of the data built into them, less energy needs to be spent on learning those symmetries. If rotational invariance is already built into a model, for example, an image recognition program would not need to be trained on rotated images, since it will already recognize all rotations by design. Ideas from the paper could be used to further improve the project's energy efficiency. This could be done by implementing the architectural design decisions mentioned above.

As with the previous paper, I will finish this section by discussing how my research could be adapted to enhance AI engineering in the context of this paper. There are several ways in which my research could be adapted. For one, my research does not prioritize energy efficiency of AI models, but rather focuses on the performance and underlying mathematical structures. By focusing more on energy efficiency, this could help making neural network models consume less power. As far as I know, neural ODEs have not been looked at specifically in the context of green AI, and this opens up a new and exciting research topic. Such a topic could include further mathematical work focusing specifically on energy efficiency of neural ODEs. One could combine the theory of ODEs with mathematical optimization in order to find the least energy cost for neural ODE training.

References

[1] Boming Xia, Qinghua Lu, Liming Zhu, Sung Une Lee, Yue Liu, and Zhenchang Xing. Towards a responsible ai metrics catalogue: A collection of metrics for ai accountability, 2024. URL `https://arxiv.org/abs/2311.13158`.

[2] Francisco Durán, Silverio Martinez-Fernandez, Matias Martinez, and Patricia Lago. Identifying architectural design decisions for achieving green ml serving. In *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering - Software Engineering for AI*, CAIN 2024. ACM, April 2024. doi: 10.1145/3644815.3644962. URL `http://dx.doi.org/10.1145/3644815.3644962`.