Software Engineering Assignment
WASP Course 2024

Matthias Möller

September 3, 2024

Task

This assignment requires you to write an essay on Software Engineering for AI/AS ("AI Engineering"), how it relates to your research, and how you can apply SE principles and tools in your project / on your sub-topic. Please only use diagrams/illustrations if necessary, and do not count these towards the length of the essay. The essay should be a minimum of 3.5 A4 pages in length, and a maximum of 5 A4 pages in length, excluding references. The font should be Times New Roman (or equivalent) and 11 point. Be sensible in formatting / layout choices.
The essay should be structured as follows:

1. Begin with an introduction/abstract to your research and topic area. This should be a maximum of 400 words, and should provide (just) enough basis so that your answers to the questions below can be understood.
2. Select at least 2 principles/ideas/concepts/techniques from Robert's lectures and discuss how they relate to your research and topic area.
3. Select at least 2 principles/ideas/concepts/techniques from the guest lectures and discuss how they relate to your research and topic area.
4. Find two full/long papers published in one of the CAIN conferences (3 have been held so far, all linked from https://conf.researchr.org/series/cain Links to an external site.), download and read them and then write in your assignment, for each paper:
   (a) Describe the core idea(s) of the paper and why it/they are important to the engineering of AI systems
   (b) How the paper relates to your own research
   (c) How your research and its results would fit into a larger AI-intensive software project where one of the core ideas from the paper would benefit the project if applied. Describe both how the paper could help improve the project and how your WASP research would fit into the project.
   (d) Discuss briefly how your research could be potentially adapted/changed to make AI engineering in the project based on the idea of the paper even better/easier.

Your answers to question 4 is the main part of your essay and should be approximately 2 A4 pages in length, 1 page per paper

Summary

My research centers around combining induction of logic programs and neurosymbolic (NeSy) AI. NeSy AI deals with integrating formal logic and neural networks (NNs). In my particular case, NeSys AI addresses approaches which use NNs to predict a symbol being true. Based on the probabilities of all neural classifiers, a single success probability for the logic program can be computed. More recent results in NeSy AI have shown that NNs can autonomously learn to extract useful features to support the correct evaluation of the logic program. In other words, the NN learns whatever it takes to support the logic program.

My particular topic centers around constructing the logic program and training the NNs at the same time. Some benefits are that the resulting systems are easier to understand by humans, while the NNs can later be inspected on which features they learn. In this respect, it provides a possibility of generating sustainable knowledge while also exploring relationships between data. Another advantage lies in the modularity of those models. A single induced model is a composition of smaller models. Where each part can be replaced, fine-tuned or removed.

Topics from Robert's Lecture

A recurring theme in the lecture are challenge resulting from the black box behaviour of pure function approximators like NNs like

- **ensuring and setting requirements** like safety, transparency, explainability and consistency (VL4, page 8-9, page 14)
- the **assessment** (value of learning, long-term potential), **contain** (i.e. explainability and accuracy) and the **integration** (i.e. continious experimentation) of AI systems (VL. 3, page 23)

NeSy AI provides a good approach to address those challenges. The logic program that leads the NN in training and inference is readable by humans. It can easily be adapted and allows for an intermediate intervention of humans into the internal computations of the system. Additionally, the potential cause for a misbehavior can be easier traced in NeSy systems than in pure black box systems. Logic programs are decomposable, modular structures and their different components can be evaluated independently. Thereby, potential errors can easier be isolated, detected and modified by humans.

Another deeply related theme is the need of diversity in knowledge and experience in teams that construct NeSy systems. As previously mentioned, NeSy systems operates on knowledge expressed in formal logic. Therefore, humans have to express this knowledge to provide a good context for the system to operate and train. To develop those systems, a well-functioning operational structure needs to be given. Bias (let it bet anchoring, availability or confirmation bias) will have an immediate effect in the development of those systems. It can be speculated that these systems are more endangered by subjective bias than purely data-driven approaches because they are directly on human knowledge. Therefore, a diverse team with different perspectives and experiences are needed to develop those systems.

Topics from Guest Lecture

We will only consider the lecture from Saab because the other one was not uploaded.

Throughout the guest lecture, we are confronted with several challenges in developing Machine Learning (ML) that results from the aspect that these systems are monolithic: 1) the creation of a complex ATM system requires the collaboration of several software engineers which requires a structural approach. Assumable, managing so many people needs a well-adjusted time management and is more complex when the system is monolithic (automatic) which results in more costs. 2) The costs for meeting requirements is increased in a monolithic system. Requirements can often only be checked with finished ML systems. However, monolithic systems become increasingly large what results in an increased need of computational resources (time and energy). As a result, the investment for developing those systems in safety-critical applications like ATM increases significantly which is supported by SAAB overinvesting in artificial intelligence (AI). Our work could address some issues because it introduces a modular (decomposable) approach. In a modular approach, requirements could potentially be checked on parts of the system and the development process could be separated into subcomponents distributed over several teams. This would allow for an easier separation of responsibilities and a sustainable development process.

A system induced with our approach could also emphasize the importance of behavioural software engineering (BSE). The aspects of our work learning modular systems and including knowledge bases results in new advantages and challenges. 1) We can include knowledge of humans in the learning. That, of course, relates to advantages and disadvantages that we

listed in the previous section. 2) Because responsibilities can be easier separated, it could be easier to gain insights about the group dynamics. People that do not work effectively could be separated into different teams which could impact the efficient development.

Task 4: Papers

What About the Data? A Mapping Study on Data Engineering for AI Systems

The paper [1] is a meta study centering around trends addressed in research related to data engineering in AI. Good data is the central element of modern AI models and requires data engineering for sustainable developments. However, this data engineering has been neglected for the most part in science. The main contribution is the identification of trends and topics that are addressed in the limited number of works available. The work identified in their analysis general workflows, technical solutions supporting AI data engineering (i.e. supporting tools, techniques for identifying outliers), architectures that are proposed for connecting the data engineering and production layer or which lessons could be learned in those papers.

NeSy AI, induction of logic programs and the modularity of our research provides interesting opportunities related to AI data engineering. Our work centers around finding relationship between vectorized data where sub-structures learn to extract sub-symbolic features to solve a task. Every module learns its features independently and exploring which features are learned from the input can result on the data engineering layer. Modules could be used to add symbolic features to the raw data in the data engineering layer. As a result, potentially defect data can be easier detected and new labels for data could be created resulting in new datasets. It could result in a feedback loop between data engineering and ML engineering resulting in a mutually beneficial relationship.

A general idea for a AI project could be the development a framework that enhances potential synergies between our work, the data engineering and the machine learning processes. For instance, an UI interface that shows images and predicted classes of an induced model would already enhance the cooperation between ML engineers and AI data engineers. ML engineers and AI data engineers could cooperate to assign the predicted class to a specific feature. By doing so, one could improve the dataset, identify which sub-structures of the logic program could be trained in isolation and generate more insight in the data itself. Further, it could help to identify noise in data.

A Meta-Summary of Challenges in Building Products with ML Components – Collecting Experiences from 4758+ Practitioners

The paper [2] is like the previous paper, a meta-study. This study centers around the general problems resulting from integrating ML and software engineering (SE). For that purpose, this study collected 50 papers and analyzed those. It discusses 6 challenges that SE encounters by integrating ML: 1. **Requirements Engineering**, 2. **Architecture, Design, and Implementation**, 3. **Model Development**, 4. **Quality Assurance**, 5. **Process**, 6. **Organization and Teams** . Thus, it provides central aspects in the challenges that should be addressed when developing AI models.

Like discussed in previous sections of this work, several problems result from most models being monolithic, completely data-driven (no human knowledge) and require many resources. NeSy AI addresses issues related to understanding a model and decreases the need of data while the modularity of our structures can address issues like the need of resources, better team management and a better sustainable development cycle.

Developing a library and framework that allows for better collaboration in a team (i.e. sharing of findings or extension of knowledge bases by non-programmers) or tools that support the inspection of our trained structures could address several challenges listed in this work. Our work centers around systems that are decomposable. Every sub-part of the system can be inspected which results in a better opportunity to guarantee aspects of fairness. I.e. if engineers find a subcomponent of our model to identify the sex of a person, the sub-structure can be fine-tuned to work well on white and black people to the same extent. Another interesting prospect is that our models allow for integrating knowledge bases (human knowledge). The knowledge base restricts the ML in their computations which can be seen as a form of guarantee. Further, because knowledge bases can be understood by non programmers, the integration of knowledge can involve several non-developers which increases diversity in teams. By providing enough resources, one could effectively create a pipeline for the sustainable development of ML models.

My research establishes a library for training and running my induced structures. This library could be combined to create the mentioned framework. UI elements that use the functions and classes provided by this library could result in a front-end which allows for the better creation. If the whole project is open-source, people would be more inclined in contributing to my established library and the UI.

References

[1] P. Heck. What About the Data? A Mapping Study on Data Engineering for AI Systems. In *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering - Software Engineering for AI*, pages 43–52, Apr. 2024. doi: 10.1145/3644815.3644954.

[2] N. Nahar, H. Zhang, G. Lewis, S. Zhou, and C. Kästner. A Meta-Summary of Challenges in Building Products with ML Components – Collecting Experiences from 4758+ Practitioners, Mar. 2023.