

User-friendly Machine Learning

Angela Barriga

Western Norway University of Applied Sciences
Bergen, Norway
abar@hvl.no

Abstract. ML is a really promising technology, yet, to apply and build a ML system, it is necessary to possess a complex skill set. The objective of this research is to reduce this complexity, establishing the guidelines to create a framework to make ML more accessible and interpretable for domain experts without data-science expertise. Reducing its learning curve would lead to a great improvement in the development of this field, democratizing its use. In this research, different fields are explored: HCI, AutoML and XAI.

Keywords: Accessible, Automated Machine Learning, Explainable Artificial Intelligence

1 Introduction

Machine Learning (ML) has risen as one of the most popular technological areas, due to its usefulness in a broad range of domains, allowing the automation of problems difficult to solve by humans. Despite its popularity, ML is not yet an accessible field to domain experts without data science knowledge, owing to the complex skill set required to use it and to interpret its results.

Democratizing and lowering the accessibility threshold of complex technologies have proven to increase their use and research efforts. Abstracting unnecessary technical details for the user by using Human Computer Interaction (HCI) techniques, adding a intuitive User Interface (UI) or following a human centred design process can be good approaches in tackling this complexity issue. Some successful examples are visual programming for controlling drones [10] or use of Lego blocks in robotics [5]. ML could make use of these approaches to be transformed into an easier to access field.

Much of the complexity for ML users lies on finding which algorithm provides the best solution for a particular problem and how to tune its hyperparameters. Automated Machine Learning (AutoML) frees users from this selection and tuning [3] by following a ML-based solution, thus reducing the amount of knowledge needed to use ML.

Another challenge for accessibility is that ML models are many times non-intuitive, and difficult for people to understand [4]. Users get results without knowing why, since algorithms do not provide any reasoning behind their output. Explainable Artificial Intelligence (XAI) aims to break this black-box nature

of ML algorithms by providing results together with explanations. This could increase ML trustiness in domains with really sensitive data (such as healthcare), and empower novice users with easier to understand algorithms and further data insight.

2 Related Work

The rise of ML has led to the appearance of different user-friendly ML tools, both commercially and in research projects.

Some of them focus on providing accessible ML solutions for domain experts in specific fields. SubCons [9] is an example of a web-based server in where subcellular researchers can perform ML operations thanks to an intuitive UI, while other example can be found in [2] where ML can help cyber security experts.

Other projects focus on transforming some ML algorithms with HCI and UI, making them easier to use. Both commercial and academic examples can be found in [6] and Lobe (<https://lobe.ai/>) which provide visual tools to work with deep learning networks.

Most efforts aim to build more general tools, not only for one specific domain or algorithm. An increasing number of companies are trying to make ML more accessible, some of them giants in the technological industry (Microsoft Azure, Amazon Web Services, Google Cloud, IBM Watson...) and other small startups, for example H2O (<https://www.h2o.ai/>) or BigML (<https://bigml.com/>).

Some remarkable projects in academia are Orange [1], a drag-and-drop visual ML environment and PennAI [7] a user-friendly Artificial Intelligence (AI) system making use of genetic programming.

Although some of these tools are really good at some of their functionalities (e.g., offering end-to-end solutions or cloud computational power), it is arguable than any of them provide ML with true accessibility. Whereas they lower the amount of ML expertise needed, many of them still require a deep knowledge of the field, since they do not hide any technical jargon and they use black-box algorithms. Commercial tools are not suitable for individual researchers nor general domain experts due their cost and also they use to suffer from vendor-locking. Finally, some of them are not intuitive to use and require an extra effort from users to learn how to use them.

3 Aims and objectives

The aim of this project is to identify what is necessary to achieve accessibility in the ML field and to apply such discoveries in building a user-friendly ML framework. Understanding and improving human performance on this field.

Taking as a starting point the accessibility already achieved in other technologies (as the examples in 1) it can be inferred that accessibility comes by reducing the entry level to a technology by minimizing the knowledge needed to work with it as well as maximizing transparency on its processes and results.

Taking advantage of already widespread HCI techniques to deliver high-quality UI and User Experience (UX) is a good high-level solution to tackle the reduction of knowledge needed. However, given the extra complexity the ML domain has with algorithm selection and hyperparameter tuning, it is necessary not only to provide users with a nice interface, but also with mechanisms to abstract these complex processes. AutoML techniques are promising to reach this desired automation.

On the other hand, XAI can be the solution to provide transparency and breaking black-box algorithms. Lime [8] is an open-source Python library that provides numerical and visual explanations of some ML algorithms results. Displaying these result descriptions and transforming them so that they can be interpreted by users without data science expertise is another objective of this project.

Although at the moment research focus is on HCI, AutoML and XAI it is expected that more decisive factors for enhancing accessibility can be discovered among the development of this project.

The final objective is to reach at least, the same degree of performance and success with the framework than with traditional ML approaches.

4 Approach

This project follows a design science methodology. Firstly, a gap in the state of the art of ML has been identified (lack of user-friendly tools providing accessible ML) by analysing relevant literature and more than 20 ML tools available online. From it we develop knowledge (how to make ML more accessible) by building and validating an artifact (accessible ML framework).

The building of said artifact is being tackled by following an incremental development approach, prototyping and iteratively adding new functionalities to the project. Consequently, the prototype will reflect the findings from research as they are found, scaling up iteration by iteration. At the moment, three techniques has been identified as useful for achieving ML accessibility and applied to the prototype: HCI design, AutoML and XAI. the prototype's ML system is built by using Scikit-learn, an open source library for Python.

In order to completely evaluate the prototype it is considered necessary to test it with different domains in real environments, not only in the academic. Connection with real world is of utmost importance in a human-centred project like this. ML competition websites and OpenML (www.openml.org) offer real datasets from trusted sources, ideal for initial testing. More definite evaluation will be done by designig experiments with subjects from different domains, with diverse degrees of data-science expertise. We consider e-Health and Smart City especially interesting domains for case studies since the sensitive nature of their data would be perfect to show the possibilities XAI opens.

The evaluation will be measured by comparing the performance of the artifact in comparison with traditional ML approaches by using the same data. During the experiments, different features will be taken into account, such as: capacity

of the user to work with the framework without any extra guidance, adaptability of the tool regarding the problem to solve, overall performance, obtained results, ability to actually solve the problem proposed, approximation of the time saved using the tool in contrast with traditional ML development and direct feedback, suggestions or feelings from the user. As a result, the general performance of the framework will be analysed, validating whether it had reached its goals or not and improving it if necessary with each development iteration.

5 Conclusions

This project focus on making ML a more accessible field for domain experts without data-science expertise. Following a design science methodology, this reserach will produce an artifact, a software tool built guided by the ideas of reducing the level of knowledge needed to work with ML and increasing its results interpretability.

References

1. Demšar, J., Zupan, B., Leban, G., Curk, T.: Orange: From experimental machine learning to interactive data mining. In: European Conference on Principles of Data Mining and Knowledge Discovery. pp. 537–539. Springer (2004)
2. Feng, C., Wu, S., Liu, N.: A user-centric machine learning framework for cyber security operations center. In: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). pp. 173–175 (July 2017)
3. Feurer, M., Klein, A., Eggenberger, K., Springenberg, J., Blum, M., Hutter, F.: Efficient and robust automated machine learning. In: Cortes, C., Lawrence, N.D., Lee, D.D., Sugiyama, M., Garnett, R. (eds.) *Advances in Neural Information Processing Systems* 28, pp. 2962–2970. Curran Associates, Inc. (2015)
4. Gunning, D.: Explainable artificial intelligence (xai). Defense Advanced Research Projects Agency (DARPA), nd Web (2017)
5. Herber, P., Klös, V.: A multi-robot search using lego mindstorms: An embedded software design project. *SIGBED Rev.* **14**(1), 61–70 (Jan 2017)
6. Klemm, S., Scherzinger, A., Drees, D., Jiang, X.: Barista - a graphical tool for designing and training deep neural networks. *CoRR* **abs/1802.04626** (2018)
7. Olson, R.S., Sipper, M., Cava, W.L., Tartarone, S., Vitale, S., Fu, W., Holmes, J.H., Moore, J.H.: A system for accessible artificial intelligence. *CoRR* **abs/1705.00594** (2017)
8. Ribeiro, M.T., Singh, S., Guestrin, C.: "why should I trust you?": Explaining the predictions of any classifier. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, CA, USA, August 13–17, 2016. pp. 1135–1144 (2016)
9. Salvatore, M., Shu, N., Eloffson, A.: The subcons webserver: A user friendly web interface for state-of-the-art subcellular localization prediction. *Protein Science* **27**(1), 195–201 (2018)
10. Tilley, E., Gray, J.: Dronely: A visual block programming language for the control of drones. In: *Proceedings of the SouthEast Conference*. pp. 208–211. ACM SE '17, ACM, New York, NY, USA (2017)