XAutoML: A Visual Analytics Tool for Establishing Trust in Automated Machine Learning

MARC-ANDRÉ ZÖLLER*, USU Software AG, Germany
WALDEMAR TITOV, Institute of Ubiquitous Mobility Systems, Karlsruhe University of Applied Sciences, Germany
THOMAS SCHLEGEL, Institute of Ubiquitous Mobility Systems, Karlsruhe University of Applied Sciences, Germany
MARCO F. HUBER, Institute of Industrial Manufacturing and Management IFF, University of Stuttgart, and Center of Cyber Cognitive Intelligence (CCI), Fraunhofer IPA, Germany

In the last ten years, various automated machine learning (AutoML) systems have been proposed to build end-to-end machine learning (ML) pipelines with minimal human interaction. Even though such automatically synthesized ML pipelines are able to achieve a competitive performance, recent studies have shown that users do not trust models constructed by AutoML due to missing transparency of AutoML systems and missing explanations for the constructed ML pipelines. In a requirements analysis study with 26 domain experts, data scientists, and AutoML researchers from different professions with vastly different expertise in ML, we collect detailed informational needs to establish trust in AutoML. We propose XAutoML, an interactive visual analytics tool for explaining arbitrary AutoML optimization procedures and ML pipelines constructed by AutoML. XAutoML combines interactive visualizations with established techniques from explainable artificial intelligence (XAI) to make the complete AutoML procedure transparent and explainable. By integrating XAutoML with JupyterLab, experienced users can extend the visual analytics with ad-hoc visualizations based on information extracted from XAutoML. We validate our approach in a user study with the same diverse user group from the requirements analysis. All participants were able to extract useful information from XAutoML, leading to a significantly increased trust in ML pipelines produced by AutoML and the AutoML optimization itself.

CCS Concepts: • Human-centered computing → Visualization systems and tools; Empirical studies in visualization; Visual analytics; Interactive systems and tools; • Computing methodologies → Machine learning.

Additional Key Words and Phrases: Automated Machine Learning, AutoML, Explainable AI, XAI, Transparency

ACM Reference Format:
Marc-André Zöller, Waldemar Titov, Thomas Schlegel, and Marco F. Huber. 2022. XAutoML: A Visual Analytics Tool for Establishing Trust in Automated Machine Learning. 1, 1 (February 2022), 34 pages. https://doi.org/010.1145/1122445.1122456

*Corresponding Author

Authors` addresses: Marc-André Zöller, marc.zoeller@usu.com, USU Software AG, Rüppurrer Str. 1, Karlsruhe, Baden-Württemberg, Germany, 76137; Waldemar Titov, waldemartitov@h-ka.de, Institute of Ubiquitous Mobility Systems, Karlsruhe University of Applied Sciences, Moltkestr. 30, Karlsruhe, Baden-Württemberg, Germany, 76133; Thomas Schlegel, thomas.schlegel@h-ka.de, Institute of Ubiquitous Mobility Systems, Karlsruhe University of Applied Sciences, Moltkestr. 30, Karlsruhe, Baden-Württemberg, Germany, 76133; Marco F. Huber, marco.huber@ieee.org, Institute of Industrial Manufacturing and Management IFF, University of Stuttgart, and Center of Cyber Cognitive Intelligence (CCI), Fraunhofer IPA, Nobelstr. 12, Stuttgart, Baden-Württemberg, Germany, 70569.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2022 Association for Computing Machinery.

Manuscript submitted to ACM
1 INTRODUCTION

Machine learning (ML) has become a vital part in many aspects of daily life. Yet, building well-performing ML applications is a challenging and time-consuming task that requires highly specialised data scientists and domain experts. The limited availability of data scientists slows down the further dissemination of ML. AutoML aims at improving the current approach of building ML applications in two aspects: (1) ML experts can benefit from automating tedious tasks, including hyperparameter optimization (HPO), leading to higher efficiency and greater focus on more challenging tasks; and (2) domain experts can be enabled to build ML pipelines on their own without having to rely on an ML expert. In the beginning, AutoML was only used for a few aspects of the data science endeavour, e.g., tuning the hyperparameters of a classification algorithm. More recently, huge improvements have been made that enable users to automate the complete process from data encoding, preprocessing, and feature engineering to model building. Lately, researchers have proposed many new approaches for AutoML, which have reached astonishing performances, e.g., [1, 21, 23, 54]. With the ever-increasing degree of automation, understanding and validating the behaviour of AutoML systems becomes inherently more difficult. Although multiple commercial solutions have been released in the past years, e.g., [12, 15, 32], AutoML is still primarily an active research topic and only has a niche existence in the larger ML universe [30].

Currently, AutoML is only seen as a tool aiding human users during their ML endeavour in an interactive fashion [76]. However, current implementations are not designed with human interaction in mind. From a user’s perspective, AutoML systems are a black-box that creates another black-box, namely the ML pipeline, promising to solve their prediction problem. They behave in a take-it-or-leave-it manner without providing users sufficient information about the optimization procedure or the resulting ML pipelines. Without sufficient information, users cannot make an informed and accountable decision: about whether an ML pipeline created via AutoML should be used at all. During their optimization procedure, a multitude of ML pipeline candidates are generated that are all able to solve the given task. However, AutoML systems tend to create extremely diverse candidates with no significant performance differences [80]. Validating and selecting a model from the abundance of provided solutions is a time-consuming task, even for seasoned ML practitioners. For domain experts with no expertise in ML, this task is practically impossible. Furthermore, modern AutoML systems build long and arbitrarily complex ML pipelines by selecting from dozens of ML primitives—each tunable by multiple hyperparameters—, making it inherently impossible for humans to grasp the complete, high-dimensional search space. In combination with the black-box nature of many AutoML systems, it is nearly impossible to understand what is going on during the optimization procedure. This lack of transparency and explainability severely limits the trust in AutoML [14, 19, 44, 73]. Furthermore, this makes the application of AutoML for automated decision making in high-risk domains, like healthcare or finance, impossible.

In this paper, we propose a new visual analytics tool titled eXplainable Automated Machine Learning (XAutoML) for analysing and understanding ML pipelines produced by AutoML systems. This visualization aims to empower all user groups of AutoML, namely domain experts, data scientists, and AutoML researchers, by (1) making the internal optimization procedure and search space of AutoML systems transparent and (2) providing enough information to validate and select automatically synthesized ML models quickly. By combining existing techniques from explainable artificial intelligence (XAI) and visualizations tailored to AutoML, XAutoML provides a holistic visualization that makes the performed optimizations transparent and the synthesized ML models explainable. Users can compare pipeline candidates, analyse the optimization procedure independent of the actually used AutoML system to gain process insights, inspect single ML models to gain data and model insights, and inspect ML ensembles, which are often produced during the AutoML optimization. XAutoML is integrated with JUPYTERLAB [61] to blend with the usual data
science workflow. It provides measures to import the result of an AutoML optimization and export analytical results directly to Jupyter for further manual analysis.

The contributions of our work are summarised as follows:

- XAutoML is the first visual analytics tool for AutoML aimed at establishing trust. By combining existing visualization techniques with methods from XAI, XAutoML can visualize different aspects of the underlying AutoML system as well as the generated ML models in a single holistic framework. It is the first system covering data, model, and process insights all at once. In contrast to existing visual analytics tools for AutoML, XAutoML is not designed for a specific user group but is a toolbox containing information for different user groups.
- In semi-structured interviews, the informational needs of 26 domain experts, data scientists, and AutoML researchers for establishing trust in AutoML are gathered. This is the first structured evaluation of requirements of domain experts for AutoML systems at all.
- We introduce two new visualizations to explain aspects of the AutoML optimization procedures for users with minimal AutoML knowledge. In combination with improved existing visualizations, XAutoML is able to visualize all important aspects of the optimization procedure of state-of-the-art AutoML systems.
- We perform a user study with the same diverse user group from the requirements analysis to validate XAutoML. The study proves that XAutoML is usable and useful for participants from the three different user groups and helps establishing trust in the ML models created by AutoML. Participants highlighted the benefits of integrating the visual analytics with JupyterLab.

The paper is structured as follows: Section 2 introduces related work. In Section 3, requirements for XAutoML are collected based on interviews with potential users and a literature review, followed by the actual design of XAutoML in Section 4. The intended usage of XAutoML is highlighted by case studies in Section 5 and evaluated in user studies in Section 6. The paper closes with a discussion in Section 7 followed by a brief conclusion.

2 RELATED WORK

Our work on visualizing and explaining the decision-making of AutoML systems builds upon a significant amount of related work in the areas of trust in artificial intelligence (AI), XAI and AutoML. Additionally, already existing visual analytics tools proposed for AutoML are introduced.

2.1 Trust in Artificial Intelligence

The issue of defining trust has been discussed in many research areas, for example, psychology and management. For this work, we follow the definition of trust provided by Lee and See [43]: trust is “the attitude that an agent will help achieve an individual’s goals in a situation characterised by uncertainty and vulnerability”. According to Siau and Wang [68], trust of a human in an AI system depends on various factors. Some of those factors—like perception or reviews of other users of an AI system—cannot be affected immediately as they rely on external aspects over which we have no control. However, we have immediate control over the factors transparency and explainability and can improve these. To trust AI applications, humans should be able to observe the internals of an AI system and the AI system should justify its decisions, behaviours, and certainty [79]. In the context of AutoML, both AutoML itself as well as the generated ML pipeline are AI systems that have to be trusted. Consequently, these transparency and explainability factors have to be applied to both AI systems.
Several recent studies have revealed that data scientists do not trust AutoML systems [14, 19, 73, 76]. Even though participants acknowledged that such systems were able to provide high quality solutions [73], they refused to use them as they do not want to be accountable for a model they do not understand [19]. Furthermore, data scientists even argued that AutoML should be limited to people with ML knowledge, to prevent people from "automating bad decisions" [14]. Interestingly, participants of all referenced studies named the limited transparency as well as missing explanations of the final ML model as the main reasons for their limited trust.

### 2.2 Explainable Artificial Intelligence

XAI is the research area concerned with explaining AI systems in a way that can be understood by humans. Usually, automated decision making systems and ML models do not operate in a vacuum; rather they, at least to some extent, have to cooperate with human users. For ML models to be relevant and helpful, humans have to accept decisions made by those models. Yet, humans have the desire to understand a decision or get an explanation because they do not tend to trust decisions made by others blindly. This directly conflicts with the black-box nature of modern ML systems.

Consequently, establishing trust in an AI system is an important motivation for explainability [9]. In the following, several XAI techniques are introduced shortly.

ML can be restricted to models that are inherently interpretable, meaning that the reasoning of a model as a whole can be understood by humans in a reasonable time [47], removing the black-box nature of ML completely. This requires the model to be transparent and the mapping of data inputs to predictions to be comprehensible [17]. Unfortunately, interpretable models, like linear models, usually perform worse than black-box models like support-vector machines (SVMs) or artificial neural networks, implying a trade-off between explainability and accuracy [9, 24].

Instead of relying on interpretable models, surrogate approaches explain an arbitrary black-box model by producing similar predictions using an interpretable model. Global surrogates are trained to approximate a black-box model on the complete input space [52], for example approximating an artificial neural network with a decision tree [66]. In contrast, local surrogates are only valid for single data instances and their direct vicinity. Consequently, only local insights of a black-box ML model can be obtained.

As an alternative to explaining the black-box model, XAI techniques can also be used to explain the relation of input features to the dependent variable. Partial dependence plots (PDPs) visualize the average relation of a set of input features to the target variable marginalised over all other features [25]. Similarly, independent conditional expectations (ICEs) visualize the marginal performance of single-data instances separately [28]. Finally, permutation feature importance [7] measures the impact of single features on the predictive power of an ML model. By randomly shuffling the values of a single feature, the relation of the feature with the dependent variable is broken. As a consequence, important features should induce a large accuracy decrease of the ML model while unimportant features should not influence the accuracy at all.

### 2.3 Automated Machine Learning

The term AutoML summarizes systems and techniques that enable an automated creation of fine-tuned ML pipelines with minimal human interaction [80]. Those techniques promise to enable domain experts without knowledge of ML or statistics to build ML pipelines on their own. In addition, data scientists can increase their productivity by automating specific steps of their workflow.
In the beginning, AutoML methods covered only single aspects of creating an ML pipeline. The earliest works in AutoML focused on optimizing the hyperparameters of a single ML algorithm [5, 34]. Specialised systems only consider feature engineering [11, 38, 42] or the composition of multiple ML primitives into complex pipeline structures [18, 41]. More recently, AutoML systems that are capable of synthesising fine-tuned pipelines, including data cleaning, feature engineering, and modeling, have emerged [23, 51, 54, 70, 81].

Given an input data set, a loss function, and a predefined search space, AutoML systems use a variety of different strategies to generate ML pipelines. For example, auto-sklearn [23] uses Bayesian optimization for algorithm selection and hyperparameter optimization, TPOT [54] uses genetic programming for building complex shaped pipelines and HPO, ATM [70] combines multi-armed bandit learning with Bayesian optimization for optimizing the hyperparameters of a fixed pipeline and dswizard [81] combines Monte Carlo tree search (MCTS) for pipeline structure search with Bayesian optimization for HPO.

Modern AutoML systems incorporate many techniques from standard ML to boost the performance of the synthesized end-to-end pipelines, e.g., [2, 21, 23, 80]. Those techniques aim to either decrease the optimization duration, like hierarchical search spaces or multi-fidelity approximations, or improve the predictive performance, for example via ensemble learning. Although those techniques are helpful for the optimization, they make the optimization procedure more complex and difficult to understand.

Applying XAI techniques to AutoML has been tested in a few publications. Freitas [24] suggests restricting AutoML to only interpretable models and shows that this limitation only induces non-significant performance decreases. Yet, when complete end-to-end pipelines are synthesized, having an interpretable model does not explain the complete pipeline. AutoPrognosis [2] creates explanations of the final model using decision lists as a global surrogate. Finally, Amazon SageMaker Autopilot [15] makes the optimization procedure more transparent by exporting ready-to-use Jupyter notebooks containing models tested during the optimization.

2.4 Visual Analytics for AutoML

In the context of AutoML, two different groups of visual analytics tools exist: (1) tools for explaining the AutoML optimization procedure and (2) tools assisting a user with selecting one of the constructed ML models. Besides presenting new visual analytics tools for AutoML, recent studies have analysed the desired interactions between AutoML systems and human users. Those studies are analysed in more detail during the requirements analysis in Section 3.

Explaining the AutoML Optimization. Some AutoML systems provide basic visualizations about the optimization procedure to offer some degree of transparency. These include the performance of all tested candidates over time [1, 23] and a parallel coordinate view [37] to visualize all evaluated hyperparameters for single models [1, 29, 46, 48]. Although those methods allow the inference of valuable information for experienced users, many important details, like any information about the behaviour of the constructed pipelines, are missing.

While parallel coordinates are easy to understand for a single algorithm with a few hyperparameters, they become confusing for complete pipelines. AUTOAIViz [78] introduces conditional parallel coordinates (CPC) to visualize hyperparameters of complete sequential pipelines produced by AUTOAI [75]. By stacking parallel coordinates hierarchically, users are only presented with a limited number of axes at once, namely one axis for each step in the pipeline. Stacked axes can be expanded to reveal individual hyperparameters. ATMSeer [77] provides both transparency and controllability for ATM [70], the underlying AutoML system. Users can observe the optimization progress—selecting a classifier and optimizing its hyperparameters—and the performance of the generated ML models in real-time with different
granularity. In addition, users can control the optimization procedure and adjust the search space in-place during an optimization. **Hypertendril** [56, 57] focuses on visualizing the HPO search strategy of AutoML systems. By combining a parallel coordinates view with a scatter plot of sampled values of a limited set of hyperparameters over time, users are able to distinguish different search strategies. In addition, **Hypertendril** provides an estimate of the hyperparameter importance to guide users while adjusting the search space. All aforementioned visualization tools require a fixed pipeline structure. In contrast, **PipelineProfiler** [55] specializes on comparing different pipeline structures visually. A comprehensible visualization of different pipelines structures is provided by merging multiple structures into a single directed acyclic graph (DAG). Additionally, **PipelineProfiler** provides the option to render the visualization directly in Jupyter.

While those visualization tools provide valuable insights, there are still severe limitations: All presented frameworks can either handle different pipeline structures or provide insights for hyperparameter optimization, but considering both aspects simultaneously is crucial for modern AutoML systems. Other important aspects like ML ensembles or data inspection are completely ignored. While the integration of a visual analytics tool with a single AutoML system enables detailed inspections and control over this system, it basically prevents the application to other AutoML systems. An AutoML visualization should be compatible with multiple AutoML systems to be relevant for a wide user basis. With **XAutoML** we aim to overcome these limitations.

**Visual Analytics for Model Selection.** As AutoML systems produce numerous different models with very similar performances during their search procedure, assessing the performance and finally selecting a model is a challenging task for users. Various visual analytics systems have been proposed to assist domain experts with model selection: EMA [10], **CLaVis** [33], **Visus** [65], and **Boxer** [27] provide a ranking of evaluated candidates and options to compare the performance of multiple models using different metrics and confusion matrices. While **Boxer** especially focuses on the analysis of fairness, accountability, transparency, and ethics (FATE), EMA and **Visus** provide a front-end to guide domain experts during initial exploratory data analysis and specifying an AutoML optimization procedure. **CLaVis** focuses on comparing models using different scores like the performance or used hyperparameters. Even though those visual analytics tools provide simple performance statistics of ML models, no explanation of the actual model behaviour in terms of XAI is provided to aid users in selecting ML models for high-risk domains requiring further model reasoning [26]. **explAIner** [69] combines various explanation techniques in a single interactive user interface allowing users to explain various aspects of an ML model. Yet, **explAIner** is limited to evaluating a single model at once making it unsuited for AutoML.

Our approach not solely aims at assisting users in selecting a well-performing model, but it is also intended to provide enough information to establish trust in the selected model. This implies that model explanations should be considered as an additional factor for model selection besides the pure model performance. As those visual analytics tools are exclusively targeted on domain experts, crucial information about the ML model, like the pipeline structure, are hidden on purpose, making those tools less suited for experienced ML users. With **XAutoML**, we aim to overcome these limitations allowing users to select the aspects of a model analysis they are interested in. Finally, all mentioned papers failed to actually collect potential requirements from domain experts. We aim to fill this gap by performing a requirements analysis prior to designing **XAutoML**.
3 REQUIREMENTS ANALYSIS

We want to understand the needs for visual analytics of AutoML practitioners. Therefore, we first collect the requirements from different user groups through a literature review in combination with semi-structured interviews. Based on these results, we identify commonly requested explanations when using AutoML systems and distill them into three key analytical needs that visualization can solve. Finally, we formulate four design goals for XAutoML.

3.1 Collecting Informational Needs for Trust in AutoML

Various studies have collected potential requirements from data scientists regarding the use of AutoML [19, 45, 73, 74]. The important message from all these studies is that participants refused to use an ML model constructed by AutoML just because it performed well. Instead, further insights to validate the ML model were requested, e.g., to explain the behaviour of a model due to legal constraints. In addition, more information about the optimization procedure was desired, including information about other evaluated ML models and the internal reasoning of the optimizer. Finally, data scientists wanted to have the ability to modify the constructed ML model to adapt it to their personal preferences.

To the best of our knowledge, no study has evaluated the requirements of domain experts for using AutoML systems with or without visual analytics. Therefore, we performed a requirements analysis to collect important aspects affecting trust in AutoML from a diverse user basis covering domain experts, data scientists, and AutoML researchers.

In our study, we conducted a card-sorting exercise to understand informational needs in visual analytics for AutoML. Participants were given a set of digital cards containing explanations of and information about various parts of the AutoML optimization procedure. Each card contained a verb, i.e. "view", "know", and "compare", followed by a single piece of information related to either the AutoML system itself or the produced ML models. For example, one card stated "View statistics of input data" and another stated "View global surrogate for model". Each card was accompanied by an example visualization. Figure 1 contains the according visualizations for the previous examples.

We created 24 different cards based on similar studies for data scientists [19, 45] and requested information in interviews with AutoML users [14, 73]. These cards, denoted as R01 to R24, covered various aspects of data (examining the processed data), process (understanding the AutoML procedure), and model (explaining the ML model) insights. The complete set of cards and the raw results are available in Table 4 in the Appendix. Besides the predefined digital cards, participants were encouraged to add cards with additional information or explanations that they would be interested in. Participants were asked to rank the available cards from most to least important for establishing trust in AutoML and the models produced by it.

For this study 26 participants with a diverse background were recruited. Participants were acquired via a snowball sampling method, beginning the with colleagues involved in data science and fellow researchers. 46% of the participants...
assigned themselves the role data scientist, 42% domain expert, and 12% AutoML researcher. However, many participants also stated that a clear assignment to just one of these roles is difficult. The participants’ professions included manufacturing (34%), information technologies (27%), healthcare (23%), finance (4%), automotive (4%), graduate student (4%), and business administration (4%).

Prior to the study, participants were informed about the nature of the study and its procedure. As we did not expect all participants to have prior experience with AutoML, we provided a baseline AutoML interface based on screenshots of a commercial AutoML system excluding easily identifiable features like the company’s logo or name. We also provided an introduction to AutoML from an end-user perspective. The goal was to familiarise participants with the high-level design goals of AutoML and to generate a general understanding of how AutoML can aid them in their work.

Although participants were given the opportunity to add their own cards, only seven decided to use this option. Therefore, we first discuss the results of the pre-defined cards before considering the additional cards in more detail.

Figure 2 provides the ranking of the importance of the 24 predefined cards grouped by domain experts and data scientists. We treat data scientists and AutoML researchers as a single group for better readability and because it does not distort the results dramatically. As expected, domain experts and data scientists rank information about the final performance of a model, in textual (R17) or visual form (R18), as by far the most important information. Providing explanations for a model’s behaviour in form of local (R19) or global surrogates (R20) is the second most important kind of information. Some information, like the ability to compare different pipelines (R23), are more important to data scientists than domain experts. For the majority of cards, no clear preferences were found regarding the importance of the information we presented.

The seven additional cards cover three different topics. Five participants stated that they would like to modify candidates in-place to assess the impact of hyperparameters and different pipeline structures on the performance. Participant P5 expressed their desire to compare the created model with an analytical model, given that such a model already exists. P10 wanted to compare data produced by the different stages in an ML pipeline to validate that relevant information is still preserved.
3.2 Accommodating a Heterogeneous Target Audience

According to its self-proclamation, AutoML targets domain experts and data scientists [80]. A third (unintentional) user group is AutoML researchers and developers who spend considerable time studying various AutoML systems. Figure 2 shows that a clear distinction between the informational needs of domain experts and data scientists is not possible for most information. Even though slight differences between the two user groups are visible, those differences are often negligible or overlap significantly. Only for ten cards, a significant difference ($p \leq 0.05$) can be observed: Information about input data (R02 and R03) and data after feature engineering (R09, R10, and R11) are more relevant for domain experts. Data scientists stated they would always perform an exploratory data analysis before building models with AutoML. Therefore, they do not require this information in an AutoML visualization. Data scientists are significantly more interested in understanding and comparing pipeline structures (R13 and R23). Domain experts primarily stated that knowing which algorithms are used in a pipeline would not be helpful as the background knowledge to interpret this information is missing. For the same reasons domain experts also stated not being interested in a search space overview (R14) and search strategy visualization (R15, R16). For the remaining cards, the informational need does not correlate with the role of a data scientist or domain expert but highly depends on the knowledge background of the person. Similar results were also observed in other studies [14, 19, 73].

Current AutoML visual analytics tools always distinguish between either a domain expert, with no expertise in ML or programming, and a data scientist, who is only interested in technical model details but not the underlying domain [10, 26, 27, 33, 55, 57, 65, 77, 78]. We argue that the user basis is more diverse, with many shades between the classic domain expert and data scientist. Consequently, the visual analytics tool should not force users into either of the roles; rather, it should enable them to fully use their potential: A domain expert with no ML skills but knowledge in data visualization should be able to build their desired visualizations instead of being limited to the visual interface optimized for users with no technical experience. Instead of this one dimensional distinction of user groups, we group users based on their domain knowledge and ML expertise as displayed in Figure 3. In addition to the established terms domain expert and data scientist, we will refer to domain experts with fundamental ML knowledge as domain data scientists. If only a high expertise in ML is relevant, we will combine both users groups to (domain) data scientists. For the sake of completeness, users with neither ML nor domain expertise are denoted as citizen researchers and will not be further considered in this work. It is important to note that both dimensions are continuous and no clear distinction between the four user groups exists. A visual analytics tool for AutoML should provide, to varying extents, useful information for all user groups and users should be able to select relevant information.

Fig. 3. Different user groups of AutoML based on their domain and ML expertise.
3.3 Blending with the Data Science Workflow

To ease the use of the visual analytics tool, XAutoML should blend with the typical data science workflow. Wang et al. [76] proposed the data science workflow shown in Figure 4. This workflow contains three stages: preparation, modeling, and deployment, which can be further divided into ten steps from data acquisition to runtime monitoring and model improvement. The execution of the steps data cleaning to model validation is usually an open-ended, exploratory and iterative process [4, 10, 53] which uses ad-hoc visual analytics extensively [76]. These visualizations enable practitioners to gain insights into their data and models quickly. In recent years, Jupyter has become the de-facto standard environment for such interactive visualization tasks [19, 64].

Jupyter Notebook [39] and its successor, JupyterLab [61], are web-based programming environments that support interactive data science and scientific computing. JupyterLab is built around the idea of computational notebooks, which combine code, execution results, and descriptive texts into a single file [64].

AutoML systems aim to (partially) automate the steps from feature engineering up to ensembling in the data science workflow. If AutoML would be more commonly used, it is reasonable to assume that it would be mainly used in the context of Jupyter as all surrounding steps in the workflow are also mostly executed in it. Instead of providing the visual analytics as a stand-alone external tool, it should be integrated with Jupyter to provide a cohesive environment for users [14]. This integration has an additional advantage: Data analytics range from simple statistical analysis to advanced ML techniques. It is virtually impossible for any single visual analytics tool to cover the complete range of possible analytics. Instead of pursuing this unreachable goal, we argue to provide easy options for experienced users to extend the visual analytics with their own ad-hoc visualizations in Jupyter. To encourage such behaviour, the tool should be designed as a data pipe in the data science workflow. In contrast to a data sink that only consumes data, namely the results of an AutoML optimization, a data pipe is able to emit new data the user can continue working with. Therefore, options for exporting (intermediate) data sets and ML artifacts should be implemented. Consequently, XAutoML could blend seamlessly with the data science workflow, as displayed in Figure 4.

Although Jupyter is a mighty tool for (domain) data scientists, programming skills are required to create notebooks, which makes it to a certain degree unsuited for users with no programming skills. Following Grappiolo et al. [31], we argue that Jupyter can become a useful tool for these users if additional visualization features are incorporated into notebooks that enable them to use Jupyter. Fortunately, JupyterLab provides a powerful extension application...
programming interface (API) that allows the inclusion of interactive JavaScript applications directly into notebooks. These extensions provide the opportunity to eliminate the prerequisite of programming skills, making Jupyter a usable environment for all types of users.

3.4 Visualization Needs and Design Goals

Based on the results from the initial requirements analysis and the literature review, we formulate three visualization needs, denoted as N1 to N3, that XAutoML aims to support. In addition, four non-functional design goals, denoted as G1 to G4, are listed.

N1. Effective and Efficient Validation of ML Models. The ability to understand and validate a model produced by AutoML is crucial for the prevalence of AutoML. If users simply decide not to use it due to missing trust in the results [76], AutoML will fail to become relevant. Therefore, the foremost goal of XAutoML is to provide necessary information to quickly assess the validity of single models and support users in selecting a model from the multitude of produced ones.

N2. Understanding and Diagnosing of AutoML Methods. AutoML methods are currently often designed as black-box optimizations. To provide a better understanding and interpretation of the complex and diverse optimization strategies in AutoML, we aim to provide an effective and intuitive visualization of (1) what the complete search space looks like, (2) how pipeline structures are synthesized, and (3) how hyperparameters are optimized. This visualization shall provide a rough understanding of the underlying search algorithm, without requiring extensive knowledge in AutoML.

N3. Search Space Refinements. As shown in Section 3.3, AutoML is usually used in an iterative workflow. Between two consecutive runs of AutoML, users have the option to adapt the underlying search space that is provided as a preset before performing the optimization. To effectively choose a refined search space, users should have information about which regions of the search space perform well and which regions can be pruned.

G1. Align with the Target Audience of AutoML. AutoML is aimed to assist domain experts and data scientists. Therefore, the visual analytics should also target these two groups. In addition, AutoML researchers should be able to extract useful information from the visual analytics.

G2. Blend with the Usual Data Science Workflow. We expect visual analytics to be constantly involved in the workflow of using AutoML. Therefore, it is crucial that the visual analytics blend seamlessly with the usual data science workflow. On one hand, this implies that output generated by an AutoML system has to be transferred easily to the visual analytics tool or that perhaps the visual analytics tool can be used to start an AutoML optimization. On the other hand, this implies that it has to be possible to transfer ML models back from the visual analytics tool to the usual data science environment, namely Jupyter.

G3. Always Provide more Detailed Information. The informational need of users is diverse. Following the idea of Five Whys [67], XAutoML should provide information in a hierarchical fashion to prevent overloading users with unnecessary and undesired information. At the highest level, only very basic information should be available and users should have the option to dig deeper into certain analytics aspects to get more information. Ultimately, the visual analytics tool can not provide all the information required by a proficient user. Therefore, we aim to add options to break-out of XAutoML. This extends G2 by not only exporting selected models but also exporting artifacts related to models, e.g., intermediate data sets or sub-pipelines, for further manual inspection in Jupyter.
Fig. 5. Overview of XAutoML. (A) The visualization is integrated with Jupyter and can be accessed with a few lines of code. (B) On the left side, the optimization overview provides basic statistics about the optimization run (B1), a scatter plot of the accuracy of all candidates over time (B2), and a receiver operating characteristic (ROC) curve of selected candidates (B3, hidden). (C) The leaderboard view provides a comprehensive overview of all evaluated candidates. Users can open single candidates (C1) to reveal detailed information about them (only partially visible). In the performance details view (C2), performance metrics and basic performance visualizations are available. By clicking the Continue in Jupyter button (C3), the according information can be exported to a new Jupyter cell. (D) Users can access the search space and ensemble inspection via these tabs.

G4. Be Open to the AutoML World. The AutoML landscape is still rapidly developing and constantly shifting. To stay relevant, the visual analytics tool should not be coupled to a specific AutoML implementation. This implies that XAutoML should only depend on generic information provided by AutoML systems. Therefore, the common basis for the visual analytics and AutoML implementations should be scikit-learn [59], NumPy [71] and pandas [49], three commonly used libraries for ML in Python.

4 XAutoML: EXPLORING AUTOML OPTIMIZATIONS

To fulfill the requirements, visual needs, and design goals identified in the previous section, we developed XAutoML. The interface of XAutoML is embedded in Jupyter and consists of an optimization overview, a candidate inspection to explore individual pipeline candidates, a search space inspection to gain insights about the optimization process and search space, and finally, an ensemble inspection view. The individual views are described in more detail in the following sections. Figure 5 provides an overview of XAutoML.

4.1 Optimization Overview

The optimization overview (Figure 5, B) provides an overview of the results of an AutoML optimization on a high level, including the total optimization duration, the number of evaluated candidates, and the performance of the best candidate. In addition, basic performance visualizations, namely the performance of all candidates over time and the
XAutoML: A Visual Analytics Tool for Establishing Trust in Automated Machine Learning

number of candidates grouped by performance, are available. Users can select multiple candidates in the overview to compare their receiver operating characteristic (ROC) curves. With these views, users can quickly identify interesting models for a detailed inspection. The candidate inspection view of interesting models can be opened directly from the overview.

4.2 Validating Machine Learning Models

The leaderboard (see Figure 5, C) provides a tabular overview of all evaluated candidates. Each row displays the performance (R17), average prediction time, and a pipeline visualization of a single candidate. The pipeline visualization renders all pipeline steps as a directed acyclic graph (DAG) that enables users to identify differences between the various candidates quickly (R13, R23). Via the Continue in Jupyter button, the corresponding candidate can be exported to Jupyter.

Users can reveal more details about candidates by selecting the corresponding entries in the leaderboard (see Figure 5, C1). The candidate inspection view provides data and model transparency for a single ML pipeline. Users can find all required information to decide if the corresponding model is a “good” model worth selecting (N1). Therefore, existing XAI techniques are incorporated to provide a holistic visual user interface. Users can interactively control the level of detail they are interested in. The requirements analysis revealed no clear preferences regarding the presented information. Therefore, we decided to implement most of the model and data inspections and provide measures for users to visualize or extract the missing information on their own.

Related information is aggregated in a card with a short description (Figure 5, C2) that can be revealed by selecting it. Figure 6 provides an overview of all implemented cards which are described in more detail later in this section. Inspections in each card are always computed based on the output of a single step in the pipeline. In Figure 5, a virtual data source node is currently selected and all inspections are calculated on the input data. Users can observe how the different steps in a pipeline affect the data by selecting the corresponding nodes in the pipeline visualization (see Figure 5, C4) and inspecting the updated content of the different cards. Each card provides at least one option to export the visualized data to Jupyter. Finally, users can also compare the information presented in a single card for various models (see Figure 5, C5, R22, R23, R24).

The performance details view (Figure 6a) provides basic performance metrics (R17) and visualizations (R18). Displayed are training and validation performance, duration of the training, and duration of predicting new samples. The class report provides the precision and recall for each individual target class. Additionally, a standard confusion matrix and ROC curve are displayed. Users can export the class report and confusion matrix to Jupyter for further analysis or visualization.

The global surrogate view (Figure 6b) fits a decision tree to the predictions of the selected candidate (R19). Users can interactively control the size of the decision tree by specifying the maximum number of leave nodes, effectively weighting the explainability of the surrogate versus the fidelity to the black-box model. The fidelity bar provides an estimate of how good the decision tree resembles the actual model. Users can export the fitted decision tree to Jupyter for further analysis.

In the data set preview (Figure 6c), users can inspect the output data set of the currently selected pipeline step (R1, R5, R9). This allows users to observe how each step in the pipeline modifies the input data and provides data transparency. We deliberately decided not to support data visualizations. Study participants stated highly varying goals and desires for visualizations, covering gaining data insights, viewing statistical distributions, and generating cohorts for the analysis of FATE, just to name a few. Instead of providing only a limited data visualization—that would often be too restricted for visualizations, covering gaining data insights, viewing statistical distributions, and generating cohorts for the analysis of FATE, just to name a few. Instead of providing only a limited data visualization—that would often be too restricted for
users—, we rely on users to generate their own data visualizations in Jupyter and only provide tabular representations of the data. While this prevents users without knowledge in data visualization from visualizing the data, experienced users are not artificially limited by the visual analytics tool. Besides inspecting the tabular data, users can generate local surrogates (R20), computed via LIME [63], for arbitrary records in the data set.

The selected hyperparameters of each step in the pipeline are listed in the configuration view (Figure 6d). The hyperparameters are displayed in a CPC plot to visualize the respective search space (R14) and selected value for each hyperparameter (R21). In addition, the structure search graph at the time of sampling this pipeline structure is also displayed. More details regarding the CPC and structure search graph are available in Section 4.3.

Hyperparameters can have a significant impact on the performance of an ML model. In reality, only a few hyperparameters actually impact the performance significantly [35] making it important to identify these. The hyperparameter importance view (Figure 6e) visualizes the importance of single hyperparameters and interactions between pairs of them (N3). The hyperparameter importance is calculated using fANOVA [35]. By selecting a hyperparameter, users get a detailed overview of well- and bad-performing regions in the search space. Using these visualizations, experienced users can extract valuable insights on how to modify the search space for the next optimization round.

Manuscript submitted to ACM
Finally, the feature importance view (Figure 6f) reveals information about relevant features. Using a permutation feature importance \(^7\), the impact of each feature on the predictive power of the ML model is measured. Besides a ranking of all features, users can also view PDP and ICE plots. In case of a multi-class classification task, users can select the target class in PDP and ICE via a drop-down menu.

4.3 Inspecting the AutoML Optimization Procedure

Besides validating models produced by AutoML, gaining insights to the actual AutoML optimization procedure was ranked as a desired information during the requirements analysis. This process transparency can help users to understand what the search space looks like, how different pipelines are chosen, and which strategy is used to optimize hyperparameters (N2). Furthermore, users are given information helping them to decide if the search space was sufficiently explored and the optimization algorithm is converging to a local minimum.

Pipeline Structure Search. A multitude of different search strategies have been proposed to synthesize pipeline structures. In general, pipeline structure search approaches can be divided into three different groups: (1) The simplest approaches use a fixed pipeline structure that does not change during the optimization. Instead, only the hyperparameters of the individual pipeline steps are fine-tuned. This pipeline structure is usually hand-crafted based on best-practices. (2) Template-based approaches also utilise a best-practise pipeline, but single steps in the pipeline are restricted to a set of algorithms instead of a fixed algorithm. The optimizer is allowed to, for example, pick a classification algorithm on its own instead of only tuning an SVM. (3) Approaches in the third group are able to build pipelines with flexible shape. During the optimization, the pipeline shape can be adopted to the given problem instance freely based on some internal optimization strategy.

For a normal AutoML user, it is often not obvious what the pipeline structure search space actually looks like and how the AutoML system traverses the search space. XAutoML provides a novel, intuitive visualization that allows users to grasp the general idea of the search procedure, independent of the actual AutoML system (R15). Therefore, we iteratively merge all constructed pipelines into a single structure search graph. Using a time-lapse function, users can observe how this structure search graph is constructed iteratively and can deduct the approximate search strategy and the corresponding structure search space. Figures 7, 8, and 9 provide example visualizations for the three aforementioned search strategies.

Usually, a single ML pipeline is interpreted as a DAG in which each node is an ML primitive and edges indicate the flow of data between the primitives. ML pipelines often contain parallel paths, e.g., to use different pre-processing steps for numerical and categorical features. In the merged graph, it is not directly apparent if two child nodes of a node are actually part of the same pipeline using parallel paths or two different pipelines using identical steps at the beginning of the pipelines. A distinction between these two cases is important to correctly assess the pattern of constructed pipelines. In the case of parallel paths, we provide a visual guidance by adding the names of selected columns to out-going edges (see Figure 7).

Merging two pipeline structures to a joint structure search graph can be interpreted as a bipartite graph matching problem. To merge two DAGs \(G_1\) and \(G_2\), we use a simplified version of the graph matching algorithm proposed by Ono et al. [55]: Similar to computing the edit distance between two strings using dynamic programming, a cost matrix \(|G_1| \times |G_2|\) with all possible substitutions, additions, and deletions is constructed. Using the Hungarian algorithm [40], a mapping with minimal cost of rows to columns is computed. Two nodes are considered identical if they substitute each other, i.e., their substitution is selected in the cost matrix. \(G_1\) and \(G_2\) are merged by creating a compound node.
for identical nodes identified in the previous step and adding all remaining nodes from $G_1$ and $G_2$ to the new graph. Starting with the first two sampled pipeline structures, we repeat this procedure iteratively to merge the next pipeline structure into the joint structure search graph up to the currently selected timestamp in the time-lapse.

**Conditional Parallel Coordinates for Non-Linear Pipelines.** The conditional parallel coordinates (CPC) visualization proposed by Weidele et al. [78] provides an intuitive way to inspect the hyperparameters of a complete ML pipeline. It is an extension of the original parallel coordinates visualization [37] that allows users to interactively control the amount of information shown. Instead of showing all hyperparameters at once, CPC introduces different conditional layers of details. Users can drill down into particular steps of the ML pipeline (see Figure 10, A1), revealing more details, namely all potential algorithms that can be used in this step, in form of a parallel coordinate plot. Each algorithm can be expanded again to reveal its hyperparameters (see Figure 10, A2). This hierarchical stacking of the axes fits naturally with AutoML search spaces. Search spaces are usually defined as tree structures due to conditional dependencies between hyperparameters [36]. If, for example, an SVM is configured to use a linear kernel, the $\gamma$ hyperparameter for radial basis function kernels is inactive as it does not change the behaviour of the SVM.

The visualization proposed by Weidele et al. [78] has two limitations, preventing the usage in combination with arbitrary AutoML systems. First, CPC requires a fixed number of coordinates present in all evaluated pipelines. This implies that all pipelines have to have the exact same number of steps. To resolve this limitation, we extend CPC by...
introducing the option to not provide values for selected coordinates. These missing values are indicated by a dashed line (see Figure 10, B). Second, CPC assumes a total order of pipeline steps. Yet, in reality, pipelines often contain parallel paths to use different pre-processing steps for categorical and numerical features. We extend CPC to support non-linear pipelines by splitting the vertical space into multiple simultaneous coordinates (see Figure 10, C1 and C2) for steps containing parallel paths. Consequently, the axes in CPC align with the actual pipeline shape again.

Users can observe the hyperparameter search strategy in a time-lapse (R16, N2). To observe the sampling of individual hyperparameters, a sampling history view—inspired by the visualizations in HyperTendril [57]—can be opened by selecting specific axes (see Figure 10, D). The sampling history view, displayed in Figure 11, contains multiple plots, one for each selected hyperparameter. Each individual hyperparameter is visualized using a scatter plot: Each scatter point represents a single ML model, the $x$-axis presents the timestamp at which the model was sampled, and the $y$-axis represents the value of the selected hyperparameter. Additionally, a color scale is used to encode the performance of each evaluated model such that users can confirm the optimization is converging to a local minimum. On the right-hand side, a histogram shows the distribution of sampled values over the possible search space. By selecting a scatter point, the details for the according model can be inspected. Figure 11 contains four example visualizations for different search strategies.

Finally, we integrate CPC with the remaining user interface. Users can highlight individual candidates for a more detailed inspection by brushing numerical axes or selecting a choice in categorical axes. Further details for interesting candidates identified in CPC can be accessed in the candidate inspection view by selecting the candidate.

**Candidate Similarity and Search Space Coverage.** Current AutoML systems do not provide measures for users to estimate the optimization progress. Users usually have to provide an optimization duration before starting the optimization but have no guidance on what optimization duration is suited for their problem. An optimization duration is long enough if the search space was sufficiently explored and the optimizer converged to a local minimum. We propose a new procedure to visually inspect the coverage of an arbitrary AutoML search space, based on a non-linear metric.
Fig. 11. Visualization of different hyperparameter search strategies.

**Algorithm 1:** High-level description of the algorithm to visualize the exploration progress of the complete search space.

1. **Data:** Evaluated Candidates $\tilde{\lambda}$, Performances $\pi(\tilde{\lambda})$.
2. Hyperparameter Search Spaces $\Lambda$

   a. Merge all search spaces $\tilde{\Lambda}$ into $\Lambda_{\text{merged}}$.
   b. Create artificial boundary candidates $\tilde{\lambda}_{\text{boundary}}$ based on $\Lambda_{\text{merged}}$.
   c. For each pair $\lambda', \lambda'' \in \tilde{\Lambda} \cup \tilde{\lambda}_{\text{boundary}}$, compute the distance $d(\lambda', \lambda'')$ using Equation (1).
   d. Project $\tilde{\lambda}$ into a 2d-space using an MDS based on $d(\lambda', \lambda'')$.
   e. Fit a regression model $\hat{r} : \mathbb{R}^2 \times \pi(\tilde{\lambda}) \to \mathbb{R}$.
   f. Create performance heat map using $\hat{r}$.

Fig. 12. Visualization of the exploration and exploitation progress of the complete search space in two dimensions. Each scatter point represents a candidate, the heat map in the background provides an estimate of the performance.
Given all previously evaluated candidates, their according search space definitions, and their performances, we want to create a single plot that visualizes how well the search space was explored. As some AutoML systems use a progressive widening of the search space, e.g., [81], a support of multiple search spaces is necessary. In the first step, we reuse the algorithm to merge different pipelines presented in the previous section to merge all hierarchical input search spaces into a single DAG $\Lambda_{\text{merged}}$. All existing candidates are padded with the default value of each newly introduced hyperparameter.

Next, boundary candidates $\tilde{\lambda}_{\text{boundary}} = \{\min(\lambda_1), \max(\lambda_1)\} \times \cdots \times \{\min(\lambda_i|\lambda_i), \max(\lambda_i|\lambda_i)\}$ are created with $\min(\lambda_i)$ and $\max(\lambda_i)$ being the lower and upper boundary of hyperparameter $i$, respectively, and $|\lambda|$ being the number of hyperparameters in $\Lambda_{\text{merged}}$. For high-dimensional search spaces this step is skipped due to the combinatorial explosion of possible candidates. Next, the pair-wise distances between all candidates are calculated respecting the tree-structured search space. Therefore, we assume that the importance of a hyperparameter $\lambda_i$ is directly dependent on its depth $\delta(\lambda_i)$ in the hierarchical search space tree. The distance between two candidates is defined as a normalized heterogeneous euclidean distance weighted by $\delta(.)$ as

$$d(\lambda', \lambda'') = \sum_{i=1}^{|\lambda|} \text{dist}(\lambda'_i, \lambda''_i).$$

(1)

For a numerical hyperparameter $\lambda_i$, $\text{dist}(.)$ is defined as

$$\text{dist}(\lambda'_i, \lambda''_i) = \frac{\lambda'_i - \min(\lambda_i)}{(\max(\lambda_i) - \min(\lambda_i)) \delta(\lambda_i)} - \frac{\lambda''_i - \min(\lambda_i)}{(\max(\lambda_i) - \min(\lambda_i)) \delta(\lambda_i)}.$$

In case of $\lambda_i$ being a categorical hyperparameter, $\text{dist}(.)$ is defined as

$$\text{dist}(\lambda'_i, \lambda''_i) = \frac{1 - \mathbb{1}(\lambda'_i, \lambda''_i)}{\delta(\lambda_i)}$$

with $\mathbb{1}$ being the indicator function.

Based on this distance matrix, all candidates are mapped into a 2d-space using an MDS. Furthermore, a regression model $\hat{r} : R^2 \times \pi(\tilde{\lambda}) \rightarrow R$ is fitted on the performance of the 2d candidates. This regression model is used to create a heat map showing the expected performance of the complete search space. In combination with an interactive time-lapse, users can check the iterative exploration of the search space and the exploitation of knowledge about well-performing regions.

### 4.4 Ensemble Inspection

Many AutoML systems construct an ensemble of the best performing pipelines instead of yielding only the best candidate [23, 54, 81]. Therefore, XAutoML provides an ensemble inspection view. This view contains the previously introduced candidate inspections for the complete ensemble. In addition, two visualizations are used to aid users in assessing the ensemble quality. We provide a tabular listing of all candidates in the ensemble with the according ensemble weighting. Users can open ensemble members in the candidate inspection view to get further details about the underlying ML model. In addition, users can compare the individual predictions of all ensemble members on any record in the input data set.

Finally, we provide a decision surface plot for all ensemble members and the complete ensemble. A decision surface is a hyper-plane separating data points in the input data space according to their predicted class label. By mapping these hyper-planes into a two-dimensional space via a principal component analysis (PCA) [58] and using a color-coding for regions separated by decision surfaces, the decision making of a classifier can be visualized as a heat map. Even
though these decision surface plots only provide a very rough impression of the actual decision making of the models, users can still get an impression of how the different ensemble members behave. The decision surface plots shall enable users to quickly identify interesting ensemble members that behave differently from the rest. Those models can then be inspected in more detail.

4.5 Implementation Details

XAutoML is designed as a JupyterLab extension. The front-end is implemented in React [50], Recharts [62] and D3 [6]. The back-end, responsible for everything related to model evaluations, is implemented as a Python package using scikit-learn [59], NumPy [71] and pandas [49].

Execution results of AutoML systems—namely the fitted models, a description of the complete search space, and some minimal meta-information—can be imported into XAutoML via a small wrapper code. Supported AutoML systems are dswizard [81], auto-sklearn [23], grid and random search from scikit-learn [59], FLAML [72], and Optuna [1].

To provide a seamless integration with Jupyter the imported execution results are rendered as a custom MIME type. The Jupyter extension connects this custom MIME type with the React application. Additionally, the extension provides measures to export code snippets to new Jupyter cells which are used to extract artefacts from XAutoML and transfer them to Jupyter. Whenever the execution of Python code is necessary, e.g., for evaluating a single model, the extension provides a connection to the currently running user-kernel such that all code is executed in the same Python environment. The complete source code is publicly available on Github\(^1\) and can also be installed easily via the Python package manager.

5 CASE STUDIES

To highlight how XAutoML supports users of AutoML systems, we describe how it can be used in combination with an arbitrary AutoML system for three real-world case studies.

5.1 Case Study 1: Understanding the Generated ML Pipelines

In this case study, we illustrate how a domain expert persona named Alice, a physician with no ML expertise, can use XAutoML to analyse models generated via AutoML. Alice aims at creating a model predicting whether a patient has a high risk for a cardiovascular disease. With no prior knowledge of ML, she uses a web-based service to fit different classification models on historical records of patients she has collected. After the optimization is done, Alice is presented with a single model with 87% accuracy.

Due to the high-risk nature of misclassifications, Alice does not want to use the suggested best-performing model blindly but instead wishes to examine the produced models closely before using them. She loads the results in XAutoML to gain more insights into the generated models. At first glance, she notices that all displayed models have an accuracy between 86% and 87%. She opens the performance details for the best performing model. The first important information is the specificity and selectivity of the model. Alice reviews the confusion matrix and model report to assess the number of misclassifications. After checking that the other candidates yield similar specificity, she continues to validate that the model makes sensible decisions. Therefore, she opens the feature importance inspection and global surrogate. Alice notices that most models use an electromyography (EMG) diagram shape as the most important feature, which aligns with her expectation. The best candidate uses the patient’s sex as the second most important feature to classify a high

\(^1\)Available at https://github.com/Ennosigaeon/xautoml

Manuscript submitted to ACM
risk. She disagrees with this assessment and moves on to the second-best candidate. This model uses the presence of exercise-induced angina, which makes more sense in her opinion, so she decides to further analyse this candidate. Next, Alice takes a closer look at a few patient records. By selecting records from the data set preview with low confidence, Alice analyses why the model is not sure about the predicted class. By comparing the provided local surrogates with her background knowledge, she verifies that these particular patients have indeed no clear symptoms. Satisfied with the provided explanations, Alice decides to pick the second-best model.

5.2 Case Study 2: Steering the Optimization Procedure

Next, we illustrate how XAutoML helps a data scientist persona, to evaluate the search process as a whole and single pipeline candidates. Bob, who is a consultant developing ML models for customers, is tasked with creating an optimized ML pipeline. As usual, he starts up JupyterLab to perform an exploratory data analysis. After familiarising with the data set, Bob wants to create a set of baseline models using AutoML. He starts the optimization procedure in the AutoML system of his choice. After the optimization procedure has finished, he loads the results in XAutoML.

Bob first scans the leaderboard with all candidates and observes that the accuracy differences between the top pipelines are less than 2% and very similarly looking pipelines have been created. By comparing the different structure graphs, Bob can quickly examine which algorithms are used in the single pipeline candidates. Before exploring a candidate in more detail, he wants to examine whether enough pipeline candidates have been created and if the search space was sufficiently investigated. He switches to the search space overview and examines the explored pipelines in the CPC plot. At first, he notices that only a single pipeline using an SVM was tested. Furthermore, gradient boosting was only used without preprocessing. A glance at the 2D optimization progress view shows that all candidates are quite evenly scattered in the search space and no cluster of similar candidates was created. With this information, Bob decides that the search process was prematurely stopped and should be resumed for some more time. While checking the search space overview, he also notices that pipelines using a decision tree performed worse than the remaining candidates. Therefore, Bob decides to remove decision trees altogether. After the second optimization run, he checks the optimization progress view again and this time a cluster of similar candidates is visible. Convinced that the search procedure was performed thoroughly, he again turns to the candidate inspection.

By selecting a well-performing pipeline using a random forest from the leaderboard, the details of the according pipeline are revealed. A glance at the hyperparameter importance view reveals that the selected imputation strategy has the largest impact on the pipeline performance. Bob selects the according imputation step in the pipeline visualization and exports the intermediate data set and the isolated imputation algorithm via a single click to PYTHON code. He continues to visualize the generated intermediate data set using his known tooling in Jupyter and tests the impact of different imputation strategies on the transformed data. Satisfied with the explored hyperparameters, he decides not to start a new optimization procedure.

Bob exports the PYTHON code of the selected pipeline via a simple click and can continue directly in Jupyter. Since he noticed that some steps in the automatically generated pipeline do not modify the data set, he continues to adapt the pipeline in Jupyter manually.

\[\text{For the sake of completeness, most AutoML systems still lack the option to actually deploy models to production without programming skills. Yet, this is a technical problem that is solved by many commercial solutions, e.g., H2O.ai [32] or DataRobot [16], and is not further considered in this case study.}\]
5.3 Case Study 3: Validating the Behaviour of AutoML Methods

In the final case study, a persona named Charlie, who is an AutoML researcher, uses XAutoML to visualize and verify an AutoML algorithm under active development. This new algorithm is supposed to build pipeline structures with increasing complexity and length using MCTS. For each created pipeline, the hyperparameters are supposed to be optimized via hyperopt [5], a well-established model-based HPO algorithm. The performance of his approach is fairly good but worse than existing AutoML systems. To analyse this shortcoming, Charlie loads a recent optimization run into XAutoML and opens the search space inspection.

He examines all evaluated pipeline structures in the structure search graph. By rewinding through the complete optimization run using the time-lapse function he can examine the traversal of the search tree step by step. At first glance, the pipeline construction performs as expected and better pipelines are found over time. Next, he turns to inspecting the evaluated hyperparameters. He selects a pipeline with mediocre performance at random to check the hyperparameters of the used classifier. By opening all hyperparameters in the sampling history view he checks the sampled hyperparameters over time. Charlie notices that the hyperparameters appear to be sampled at random without converging to a local minimum. hyperopt uses Bayesian optimization to select promising hyperparameter values. This requires building an internal model of the search space based on previous observations. In the beginning, random values are sampled to build an initial model. The new AutoML system simply did not evaluate enough hyperparameters for each pipeline candidate to build an initial model and basically only used random search for HPO. Realising this, Charlie decides to increase the number of hyperparameter evaluations of each pipeline candidate to utilize the full potential of hyperopt.

6 EVALUATION

In this section, we demonstrate the usefulness and effectiveness of XAutoML in three user studies. As discussed by Muller et al. [53], many different roles are involved within data science projects. Similarly, AutoML also does not aim to support a single user group but tries to assist multiple roles. Accordingly, an evaluation of AutoML visualization methods should also be performed with multiple user groups.

6.1 Study Protocol and Participants

Each user study is aimed at a different user group, i.e., domain experts, (domain) data scientists and AutoML researchers. These studies were performed with the same 26 participants from the requirements analysis study in Section 3.1. The user studies used a semi-structured method and consisted of four major phases:

(1) The first phase is used to gain a better understanding of the participants daily work and abilities. Each participant is asked to describe their job role and their daily tasks in regard to data analysis and ML. Additionally, participants are shortly asked to gauge their proficiency with ML and AutoML on 5-point Likert scales.

(2) The second phase aims to familiarise participants with the current state-of-the-art in AutoML. Depending on their stated proficiency with ML and AutoML, participants were given a short, high-level introduction to AutoML. They were provided the typical outputs produced by state-of-the-art AutoML systems, e.g., [23, 54, 72], in a Jupyter notebook, namely a textual representation of the best pipeline, the validation loss of the best pipeline, as well as a visualization of the loss during the optimization. Based on this information, participants were asked to provide a first evaluation of their trust in AutoML to establish a baseline trust measure.
Next, participants were asked to interact with XAutoML for roughly 40 minutes. During this phase, participants were encouraged to speak while using the system in a think-aloud study, as it was done in other evaluations of visual analytics tools, e.g., [55, 57, 77, 78]. To encourage the exploration of the various aspects of XAutoML, participants were given small tasks to solve. The different tasks are described in detail in the next sections. We reused the exact same run history from the second phase for all evaluations.

Finally, the trust of the participants in AutoML methods was evaluated again using the same questionnaire as in Phase 2. In addition, the visual design and usability of XAutoML are recorded using a 5-point Likert scale. In the end, participants were asked to reflect on any information that was missing in XAutoML. Finally, liked and disliked elements of the study could be voiced, and participants were given the opportunity to provide feedback freely.

6.1.1 Domain Experts: Establishing Trust in the Generated Pipelines. In the case study for domain experts, we aim to gauge the ability of domain experts to quickly validate and select ML models using XAutoML. Particularly interesting are potential effects of information overloading [60] as domain experts are exposed to much information they can not understand, for example, the importance of hyperparameters or the search space overview.

Participants were provided with a data set tailored to their professional background, instead of participants using their personal data sets, to eliminate effects of different data sets. They were selected to be (1) a classification problem, (2) a relevant problem in the according domain, (3) not trivially-solved by an ML algorithm, and (4) simple enough to be solvable by a domain expert by hand. For example, participants with a healthcare background were asked to create an ML model predicting a high risk for a stroke based on eleven continuous and categorical features [22]. Besides the raw data, domain experts were also provided with a description of all features and were allowed to familiarise with the data set.

Afterwards, each domain expert was asked to use the visualization to validate some of the produced models. The goal was to either find a model the domain expert was willing to use or determine that the produced models are not helpful and that the AutoML optimization should be repeated. To guide the exploration of the participants, we created a set of information-retrieval tasks listed in Table 5 in the Appendix. All tasks only concerned general information provided in XAutoML or validating the behaviour of an ML model and required no specific ML knowledge.

6.1.2 (Domain) Data Scientists: Informed Usage of AutoML. In the second case study, we aim to validate that (domain) data scientists are able to find and extract useful and understandable information from XAutoML. Of special interest are the integration of XAutoML with the usual data science workflow and to which extent (domain) data scientists without prior knowledge of AutoML are able to grasp the internals of the used AutoML system.

Data scientists were asked to use XAutoML to analyse predictive models for the "Multiple Features: Morphological" data set [20]. This data set contains six unknown morphological features related to handwritten numbers. To encourage the exploration of the different views, participants were asked to solve a set of factual information-retrieval tasks involving most of the previously described views. The complete list of all tasks, including the success rate, is given in Table 6 in the Appendix. In addition, participants were given prerecorded run histories of various AutoML systems on the same data set and were asked to gain insights into the underlying AutoML system.

6.1.3 AutoML Researchers: Validating the Optimization Procedure. The user study regarding AutoML researchers differs from the previous two studies. In addition to solving the same tasks like the data scientists, researchers were asked to
Table 1. Summary of the questionnaire measuring the trust in AutoML and its generated models for domain experts (DE), data scientists (DS), AutoML researcher (AR), and all together. For each question, the two rows represent results before and after using XAutoML, respectively. Values are given on a scale of 1 (strongly disagree) to 5 (strongly agree).

| Question | Before | After | DE | DS | AR | All |
|----------|--------|-------|----|----|----|-----|
| Q11 I understand how good the selected model is. | 3.15 | 3.10 | 2.33 | 3.04 | 3.88 | 4.50 |
| Q12 I understand what the selected model does. | 3.38 | 2.80 | 1.33 | 2.92 | 4.23 | 4.70 |
| Q13 I have enough information to decide if I want to use the model. | 2.46 | 2.10 | 2.33 | 2.31 | 3.77 | 4.20 |
| Q14 I have an idea what happened during the AutoML optimization. | 1.92 | 2.90 | 2.00 | 2.31 | 2.54 | 4.30 |
| Q15 I would trust a model constructed by AutoML. | 2.54 | 2.90 | 2.33 | 2.65 | 3.92 | 3.90 |
| Q16 I think AutoML can help me in my daily work. | 3.62 | 3.50 | 3.67 | 3.58 | 4.00 | 4.50 |

6.2 Main Insights and Participant Feedback

Overall, XAutoML was able to increase the trust in AutoML systems significantly. On a scale from 1 (strongly disagree) to 5 (strongly agree), trust in ML models constructed by AutoML increased from 2.65 ± 0.89 to 3.96 ± 0.82, $p = 6.65e^{-7}$, $d = 1.52^4$ after using XAutoML. Participants attributed the increased trust to a better understanding of the generated models and insights to the underlying optimization procedure. Accordingly, participants were able to successfully extract enough information to decide whether to use an ML pipeline created via AutoML or not (2.31 ± 0.74 versus 4.00 ± 0.89, $p = 5.94e^{-10}$, $d = 2.07$). In the following, we take a closer look at how XAutoML improves process transparency and model validation. Furthermore, we discuss feedback provided by the participants. Details of all presented quantitative results are available in Table 1 and Table 2.

Validating ML Models. Participants used XAutoML extensively to validate and compare ML models. Depending on their background in ML, different explanations were utilised. Unsurprisingly, users without knowledge in ML mainly focused on the performance metrics and global surrogates to gain insights into the behaviour of models. By inspecting multiple performance metrics on the train and test data in combination with the confusion matrix, users stated they received enough information to correctly assess the performance of a model (3.04 ± 1.04 versus 4.42 ± 0.50, $p = 7.21e^{-8}$, $d = 1.70$). After picking a promising model, those users usually investigated the global surrogate to check if the model “does something sensible” (P23). Local surrogates and feature importance were consulted less often.

Experienced ML users did not focus on the global and local surrogates and feature importance. This can at least partially be attributed to the analysed data set as the meaning of features was unknown to the participants. Consequently,

---

3As some minimal wrapper logic is necessary to extract the fitted models and search space from the AutoML system, the desired systems of the participants were communicated prior to the user study and wrappers were provided by the authors.

4Given are mean ± standard deviation, the $p$-value, and the effect size in terms of Cohen’s $d$ [13].
those explanations had only minimal potential to provide new insights. Instead, participants focused more on gaining insights by inspecting the used algorithms in the different pipelines. ML practitioners liked the visualization of pipeline structures. The ability to observe changes in the data and the possibility to extract each intermediate data set were considered very useful both for “visualizing the data” (P3) as well as “pipeline debugging” (P5). Some participants were able to detect ineffective or superfluous steps in the constructed pipelines using the intermediate data sets. Consequently, all participants were able to understand the behaviour of the constructed ML models significantly better using XAutoML (2.92 ± 1.32 versus 4.46 ± 0.65, \( p = 1.21 \times 10^{-6}, d = 1.48 \)).

Understanding the AutoML Optimization Procedure. The second analytical need supported by XAutoML is aiding users in understanding the underlying AutoML search strategy and search space. Even though XAutoML was able to increase the understanding of the AutoML system (2.31 ± 1.09 versus 3.42 ± 1.17, \( p = 4.15 \times 10^{-4}, d = 0.99 \)), the results highly depend on the participant’s prior experience with ML. Users with little to no knowledge in ML had gained only minor insights into the AutoML procedures. They usually stated either missing knowledge in ML or math to understand the internals or were simply not interested in it.

In contrast, (domain) data scientists were able to gain insights into the AutoML optimization procedure. Even though they had no prior practical experience with AutoML, nearly all participants were able to correctly identify and distinguish template-based, fixed, and flexible optimization strategies for pipeline structures. Multiple users were surprised by the complexity of ML pipelines produced by some AutoML systems. “I thought AutoML is only good for hyperparameter optimization and pipeline construction is just a small extension” (P10).

Similarly, most users were able to correctly identify different hyperparameter search strategies like random search, grid search or a model-based optimization. “Observing the search in a time-lapse is extremely helpful to understand the search algorithms” (P9). The combination of structure search graph and CPC enabled users to quickly identify the hyperparameters for each step in a potential ML pipeline. Nearly all users were able to formulate a rough concept of the underlying search space.

P12, an experienced AutoML user, highlighted the usefulness of the optimization progress view for assessing the progress of the optimization run. “It is often quite hard to judge if the optimization has actually converged yet. The overview gives me this information at a glance” (P12). Yet, they also remarked that providing this information in real-time during the optimization procedure would be even more helpful. We discuss this issue of human guidance in Section 7.

AutoML in the Data Science Workflow. The integration with Jupyter and the option to export data sets and artifacts ML from XAutoML to Jupyter was received overwhelmingly positive. Only a single participant with programming skills said this integration is a “nice gimmick” (P8) while all other participants highlighted the usefulness of this feature for their workflow. “Visualizations can only offer a subset of all potential analyses. Experts with domain knowledge are able to extract more information” (P2). Many participants confirmed our intended workflow presented in Section 3.3. They stated they could imagine using AutoML for creating an evaluation baseline in a new project they would aim to improve. Visual analytics are considered an integral part of AutoML. “Just because I was able to validate results in a single case, I will not trust AutoML in general” (P1). The current integration with Jupyter and the export of various artefacts from XAutoML does not force users to adapt their usual workflow. “There is simply no reason not to use the visualization” (P14). Unsurprisingly, the integration with Jupyter was basically ignored by participants without programming skills.
Table 2. Summary of the questionnaire measuring the visual design and usability of XAutoML for domain experts (DE), data scientists (DS), AutoML researcher (AR), and all together. Values are given on a scale of 1 (strongly disagree) to 5 (strongly agree).

| Question                                                                 | DE   | DS   | AR   | All  |
|--------------------------------------------------------------------------|------|------|------|------|
| Q21 The visual design is easy to comprehend.                             | 4.15 | 4.20 | 4.33 | 4.19 |
| Q22 The visual design provides sufficient details for me.               | 4.31 | 4.50 | 4.67 | 4.42 |
| Q23 The visual design seems complete.                                    | 4.15 | 4.40 | 4.67 | 4.31 |
| Q24 The visual design helps me to decide if I should trust AutoML.      | 4.15 | 4.60 | 4.33 | 4.35 |
| Q25 The visual design is helpful for my goals.                          | 3.77 | 4.40 | 4.67 | 4.12 |

Grounding the Expectation in ML. An interesting effect we were able to observe is that participants’ proficiency in ML correlates negatively ($r = -0.31$) with the understanding of what the proposed ML model does. Without providing additional explanations, participants with a low proficiency in ML reiterated the goal of the use-case when asked if they understood what the model does instead of questioning the actual behaviour of the ML model. Even when challenging this assumption, participants were still convinced that the provided ML model would solve their task. This is a good example of the risk of potentially “automating bad decisions” [14] without noticing it by practitioners with minimal ML expertise. During the usage of XAutoML most domain experts discarded the model initially suggested by the AutoML optimizer quickly using the global surrogate and performance metrics. Consequently, domain experts were able to identify invalid models, effectively preventing this pitfall.

Validating the Behaviour of the Search Algorithm. P11, an AutoML researcher, tested XAutoML with an AutoML system building increasingly more complex pipelines over time. The system uses an $\epsilon$-greedy approach to explore new pipelines in the beginning of the optimization and picks from the already evaluated pipelines towards the optimization end. Using the time-lapse function of the structure search graph, P11 observed how during the first half of the optimization mostly new pipelines with increasing length are sampled, just as they expected. Yet, towards the end of the optimization, the search algorithm suddenly started favouring very short pipelines. Longer pipelines that were also previously evaluated are completely ignored. Confused by this observation, P11 checked the implementation of the search procedure after the user study and detected a bug enforcing the selection of the shortest possible pipeline in an exploitation step. Even though this information would have also been available by carefully studying the evaluated pipelines in the log file, XAutoML revealed this flaw in under two minutes.

Information Overload. In general, users were satisfied with the information presented in XAutoML. No participants requested additional information not available in it. On average, all user groups agreed to the statements that the visual design provides sufficient details and is complete. Even though not all information were relevant for all users, participants acknowledged the benefit of showing too much information instead of too little. “Users differ very much in their experience and knowledge. I like that people are able to pick the information they need” (P23). However, the current way of providing the information in XAutoML is suboptimal. Nearly all participants, independent of their personal background, remarked a visual information overload [60] during the first minutes of the user study. “There are too many features to grasp the complete program immediately” (P3). Yet, users were able to solve 95.2% of the given tasks indicating that they were able to find the desired information. Furthermore, on average, participants agreed to the statement that the visual design is easy to comprehend and helpful for their goals. From these apparently contradicting statements, we deduce that a better structuring of the presented information is necessary. Possible solutions are discussed in Section 7.

Manuscript submitted to ACM
**Trust in Automated Machine Learning.** XAutoML was able to improve the trust of participants in AutoML significantly (2.65 ± 0.89 versus 3.96 ± 0.82, \( p = 6.65 \times 10^{-7}, d = 1.52 \)). Furthermore, participants, on average, agreed that the visual design helped them to decide if they should trust AutoML. Both data scientists and AutoML researchers consider the visual design as helpful for their goals. In comparison, domain experts have a rather negative opinion on the helpfulness of the visual design regarding their goals. Multiple domain experts explained during the study that data analytics is a rather small part of their daily work and AutoML is only of limited use for them. Consequently, we observed the smallest improvement on participants’ assessment of the helpfulness of AutoML in their daily work using XAutoML (3.58 ± 0.95 versus 4.15 ± 0.78, \( p = 1.02 \times 10^{-2}, d = 0.66 \)). We do not consider this a shortcoming of AutoML but rather attribute this observation to our limited number of participants.

### 6.3 System Usability

The usability of XAutoML is evaluated using the system usability score (SUS) [8]. To compute the SUS, participants were asked to fill out the standard SUS survey at the end of the user study. The SUS contains ten questions participants had to grade on a scale of 1 (strongly disagree) to 5 (strongly agree) and ranks a system on a scale from 0 to 100. Our system reached 72.4 ± 13.22 points. According to Bangor et al. [3], this grades the usability of XAutoML in the upper region of OK making it acceptable. The major criticism of participants was that support by a technical person is required for using this system (5.2 of 10 possible points). However, most participants also stated that they would only require support by a technical person during the initial contact with the system and felt confident that no more support would be required after using it a few times. This assessment is supported by the fact that participants were able to solve 95.2% of the tasks in the user study.

### 7 DISCUSSION & FUTURE WORK

Study participants were interested in validating the behaviour of single ML models and/or understanding the internals of the AutoML optimization. This confirms our identified visualization needs N1 and N2. It is important to note that these two needs do not correlate with the traditional user groups of data scientists and domain experts but depend on a more diverse personal background knowledge of each participant.

Interestingly, most participants with ML expertise considered AutoML only as a baseline method for ML. Instead of using a proposed model directly, they wanted to build a custom model manually improving on the performance yielded by AutoML. A potential explanation could be that most study participants had no prior experience with AutoML and were therefore satisfied with AutoML building “good enough models” (P3) for a baseline. Finding the best possible ML model via AutoML was not a goal of the participants. Consequently, a search space refinement—and therefore identifying well-performing regions in the search space—for consecutive optimization runs was not interesting for the study participants. This contradicts our identified visualization need N3. Further research with users having a wider spectrum of prior knowledge in AutoML is necessary to validate our identified analytical needs.

Instead of designing XAutoML for a single user group, we decided to provide a lot of information and rely on users to pick the relevant and ignore the rest. The user study showed that participants from all three user groups were able to extract relevant information from XAutoML supporting our design goal G1. Furthermore, study participants having programming skills highlighted the benefits of integrating XAutoML with JUPYTER. Extracting data from the visual analytics for further manual analysis was considered an integral part for incorporating AutoML and the visual analytics into the usual workflow of the participants. This confirms our design goals G2 and G3. Finally, existing AutoML systems can be integrated with XAutoML easily as only minimal information has to be provided by the AutoML system.
supporting our design goal G4. To prove this claim, XAutoML is currently able to visualize the results of five different AutoML libraries.

P21, a domain expert, mentioned an alternative usage scenario for AutoML: Instead of using the constructed ML models for a predictive task, they think AutoML in combination with the global and local surrogates can help to "extract new knowledge" (P21) from the given data set. Without the visual analytics, they would not be able to tap into the potential knowledge extracted by AutoML.

7.1 Current Limitations

During the first minutes of the user study, many participants stated that they were overwhelmed by the amount of different information presented in the visualization. This was the major criticism of XAutoML. We tried to prevent this visual information overload by designing XAutoML to provide information in different levels of details supporting our design goal G3. Yet, apparently, the current visual design fails at this task at least partially. This initial shock was usually overcome within roughly 40 minutes of participants interacting with XAutoML. Further analysis on how to restructure the presented information and visualizations is necessary. During the study several participants proposed to add the option to configure the visual analytics tool by the user to hide irrelevant information. Alternatively, pre-defined views tailored to specific areas of interest could be created, similar to the current visual analytics approaches. Users could select areas they are interested in and add further information on demand later on. Alternatively, some participants suggested introducing additional layers to expose users to less information at once.

XAutoML is currently designed to create post-hoc explanations. Users can only analyse the results of an AutoML optimization run after it has finished. Based on the extracted insights, users can adapt the search space and data set to guide the next optimization run into the right direction. From a user’s perspective, this workflow can be cumbersome as the lengthy completion of the AutoML optimization has to be awaited. In the spirit of human-guided ML, a tight coupling between AutoML system and visual analytics is highly desirable [26] to control the optimization procedure and modify the search space in-place during the optimization. Yet, this directly conflicts with the design goal to support many AutoML systems. In addition, it exposes users to internal information of the AutoML optimizer that could be hard to understand for end-users. Further research is required to distill common user interactions with AutoML systems to a standardized framework coupling visual analytics and optimizer.

As a consequence of the post-hoc explanations and the abstraction of the underlying AutoML system, most visualizations are computed on the fly. These ad-hoc computations become quite time-consuming for large data sets, severely limiting the user experience. Even though all computed results are cached and the input data for costly operations is down-sampled, the initial computation of the requested data may still require too much time for an interactive system. Another drawback of being AutoML systems agnostic is the lack of information about the internal optimizer reasoning. XAutoML only provides visualizations based on the evaluated models over time. Given this information, users of XAutoML are able to make an educated guess about the internal reasoning of the AutoML optimizer. It would be better if AutoML systems provide more inherent information to establish trust and explain their behaviour, but unfortunately, this is simply not the case with current state-of-the-art AutoML systems.

Multiple participants remarked that relevant information, they were looking for, was not easy to find due to a discrepancy in the used terminology. XAutoML uses established terms from ML, yet participants are often not familiar with ML and use other terms for the same concept, e.g., recall for binary classification and sensitivity. The effort to mentally map to known terms made usage of XAutoML unnecessary straining for some participants.
7.2 Future Work

Currently, programming skills are necessary to access the visualization. This basically prevents users without programming skills from using XAutoML. For now, we accepted this limitation as programming skills are also necessary to actually create an AutoML optimization run to be visualized in XAutoML. We plan to overcome both limitations, by providing an option to run the visualization as a stand-alone web service and including a control plane similar to Visus [65]. This control plane could allow users to create AutoML optimization procedures and configure them accordingly through a visual user interface.

During the user study, many users voiced their desire to create specific ML models based on the insights extracted from their detailed analysis of ML models, e.g., giving a higher importance to a specific feature. Gil et al. [26] have analysed common requirements for human-guided ML. An option to incorporate human guidance into a running AutoML optimization, building single models specifically requested by the user, would be useful.

XAutoML is currently limited to classification tasks on tabular data. An extension to further learning tasks and data types is desirable and was requested during the user study by multiple participants. Similarly, we plan the inclusion of further AutoML systems to increase the potential user basis of XAutoML.

8 CONCLUSIONS

We presented XAutoML, an open-source visual analytics tool for establishing trust in AutoML procedures by making AutoML optimizations transparent and explaining ML models produced by AutoML. In a requirement analysis study, we have collected desired explanations and information from a diverse user basis containing 12 data scientists, 11 domain experts, and 3 AutoML researchers. The results indicate that designing visual analytics tools focused on a single user group is, in the context of AutoML, not helpful. A clear assignment of explanations to specific user groups is often not possible. XAutoML allows users to pick interesting information from a broad spectrum. In a user study, we were able to prove the effectiveness and usefulness of XAutoML. Our results showed, that the usage of XAutoML significantly increased the understanding of AutoML systems and ML models produced by them leading to an increased trust of users in AutoML.

ACKNOWLEDGMENTS

The authors wish to thank the participants of the requirements analysis and the user study for their time and valuable input. This work was partially supported by the German Federal Ministry for Economic Affairs and Climate Action in the project FabOS (project no. 01MK20010N), by the German Federal Ministry of Education and Research in the project RESPOND (project no. 01S8067A) and by the Baden-Württemberg Ministry for Economic Affairs, Labour and Tourism in the project KI-Fortschrittszentrum "Lernende Systeme und Kognitive Robotik” (project no. 036-170017).

REFERENCES

[1] Takuya Akiba, Shotaro Sano, Toshihiko Yanase, Takeru Ohta, and Masanori Koyama. 2019. Optuna : A Next-generation Hyperparameter Optimization Framework. In International Conference on Knowledge Discovery and Data Mining. Association for Computing Machinery, 2623–2631.
[2] Ahmed M. Alaa and Mihaela Van Der Schaar. 2018. AutoPrognosis: Automated Clinical Prognostic Modeling via Bayesian Optimization with Structured Kernel Learning. International Conference on Machine Learning 1 (2018), 139–148.
[3] Aaron Bangor, Philip T. Kortum, and James T. Miller. 2008. An Empirical Evaluation of the System Usability Scale. International Journal of Human-Computer Interaction 24, 6 (2008), 574–594.
[4] Andrea Batch and Niklas Elmqvist. 2018. The Interactive Visualization Gap in Initial Exploratory Data Analysis. IEEE Transactions on Visualization and Computer Graphics 24, 1 (2018), 278–287.

Manuscript submitted to ACM
XAutoML: A Visual Analytics Tool for Establishing Trust in Automated Machine Learning

[35] Frank Hutter, Holger H. Hoos, and Kevin Leyton-Brown. 2014. An Efficient Approach for Assessing Hyperparameter Importance. In International Conference on Machine Learning, 754–762.

[36] Frank Hutter, Holger H. Hoos, Kevin Leyton-Brown, and Thomas Stützle. 2009. ParamILS: An Automatic Algorithm Configuration Framework. Journal of Artificial Intelligence Research 36 (2009), 267–306.

[37] Alfred Inselberg and Bernard Dimsdale. 1990. Parallel Coordinates: A Tool for Visualizing Multi-Dimensional Geometry. In IEEE Conference on Visualization. 361–378.

[38] Gilad Katz, Eui Chul Richard Shin, and Dawn Song. 2017. ExploreKit: Automatic feature generation and selection. In IEEE International Conference on Data Mining. 979–984.

[39] Thomas Klayyer, Benjamin Ragan-Kelley, Fernando Perez, Brian Granger, Matthias Bussonnier, Jonathan Frederic. Kyle Kelley. Jessica Hamrick, Jason Grout, Sylvain Corlay, Paul Ivanov, Damien Avila, Safia Abdalla, and Carol Willing. 2016. Jupyter Notebooks—a publishing format for reproducible computational workflows. In Positioning and Power in Academic Publishing: Players, Agents and Agendas. IOS Press BV, 87–90.

[40] H. W. Kuhn. 1955. The Hungarian method for the assignment problem. Naval research logistics quarterly 2, 1-2 (1955), 83–97.

[41] Brenden M. Lake, Tomer D. Ullman, Joshua B. Tenenbaum, and Samuel J. Gershman. 2017. Building machines that learn and think like people. Behavioral and Brain Sciences 40 (2017), 1–58.

[42] Hoang Thanh Lam, Johann-Michael Thiebaut, Mathieu Sinn, Bei Chen, Tiep Mai, and Ozgur Alkan. 2017. One button machine for automating feature engineering in relational databases. arXiv preprint arXiv:1706.00327 (2017), 1–9.

[43] John D. Lee and Katrina A. See. 2004. Trust in Automation: Designing for Appropriate Reliance. Human Factors 46, 1 (2004), 50–80.

[44] Lisha Li, Kevin G. Jamieson, Giulia DeSalvo, Afshin Rostamizadeh, and Ameet Talwalkar. 2018. Hyperband: A Novel Bandit-Based Approach to Hyperparameter Optimization. Journal of Machine Learning Research 18 (2018), 1–52.

[45] Q. Vera Liao, Daniel Gruen, and Sarah Miller. 2020. Questioning the AI: Informing Design Practices for Explainable AI User Experiences. In Conference on Human Factors in Computing Systems. Association for Computing Machinery, 1–15.

[46] Richard Liaw, Eric Liang, Robert Nishihara, Philipp Moritz, Joseph E Gonzalez, and Ion Stoica. 2018. Tune: A Research Platform for Distributed Model Selection and Training. In arXiv preprint arXiv:1807.05118. 1–8.

[47] Zachary C. Lipton. 2018. The Mythos of Model Interpretability: In Machine Learning, the Concept of Interpretability is Both Important and Slippery. Queue 16, 3 (2018), 31–57.

[48] Jiayi Liu, Samarth Tripathi, Umesh Kurup, and Mohak Shah. 2019. Aupimizer - an Extensible, Open-Source Framework for Hyperparameter Tuning. arXiv:1911.02522 (2019), 1–10.

[49] Wes McKinney. 2010. Data Structures for Statistical Computing in Python. In Python in Science Conference. 56–61.

[50] Meta Platforms Inc. 2013. React - A JavaScript library for building user interfaces. https://reactjs.org/

[51] Felix Mohr, Marcel Wever, and Eyke Hüllermeier. 2018. ML-Plan: Automated machine learning via hierarchical planning. Machine Learning 107 (2018), 1495–1515.

[52] Christoph Molnar. 2019. Interpretable machine learning. A Guide for Making Black Box Models Explainable.

[53] Michael Muller, Ingrid Lange, Dakuo Wang, David Piorkowski, Jason Tsay, Q. Vera Liao, Casey Dugan, and Thomas Erickson. 2019. How Data Science Workers Work with Data: Discovery, Capture, Curation, Design, Creation. In Conference on Human Factors in Computing Systems. Association for Computing Machinery, 1–14.

[54] Randal S. Olson and Jason H. Moore. 2016. TPOT: A Tree-based Pipeline Optimization Tool for Automating Machine Learning. In International Conference on Machine Learning AutoML Workshop. Springer International Publishing, 66–74.

[55] Jorge Pavezint Ono, Sonia Castelo, Roque Lopez, Enrico Bertini, Juliana Freire, and Claudio Silva. 2021. PipelineProfiler: A Visual Analytics Tool for the Exploration of AutoML Pipelines. IEEE Transactions on Visualization and Computer Graphics 27, 2 (2021), 390–400.

[56] Heungseok Park, Jiwonkon Kim, Minhyu Kim, Ji-hoong Kim, Jaegul Choo, Jungs Woo Ha, and Nako Sung. 2019. VisualHyperTuner: Visual Analytics for User-Driven Hyperparameter Tuning of Deep Neural Networks. In SysML Conference.

[57] Heungseok Park, Yoonsou Nam, Ji-hoong Kim, and Jaegul Choo. 2021. HyperTendril: Visual Analytics for User-Driven Hyperparameter Optimization of Deep Neural Networks. IEEE Transactions on Visualization and Computer Graphics 27, 2 (2021), 1407–1416.

[58] Karl Pearson. 1901. LIII. On lines and planes of closest fit to systems of points in space. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science 2, 11 (1901), 559–572.

[59] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, Jake Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. 2011. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research 12 (2011), 2825–2830.

[60] Forough Poursabzi-Sangdeh, Dan Goldstein, Jake Hofman, Jennifer Wortman Vaughan, and Hanna Wallach. 2021. Manipulating and Measuring Model Interpretability. In Conference on Human Factors in Computing Systems. Association for Computing Machinery, 1–67.

[61] Project Jupyter. 2018. JupyterLab. https://jupyter.org/

[62] Recharts Group. 2015. Recharts - A Composable Charting Library Built on React Components. https://recharts.org/

[63] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. “Why Should I Trust You?” Explaining the Predictions of Any Classifier. In International Conference on Knowledge Discovery and Data Mining. 1135–1144.

[64] Adam Rule, Aurélien Tabard, and James D. Hollan. 2018. Exploration and Explanation in Computational Notebooks. In Conference on Human Factors in Computing Systems. Association for Computing Machinery, 1–12.

Manuscript submitted to ACM
Table 3. Summary of the questionnaire measuring the prior knowledge of domain experts (DE), data scientists (DS), AutoML researcher (AR), and all together in AutoML related topics. Values are given on a scale of 1 (strongly disagree) to 5 (strongly agree).

| Question | DE | DS | AR | All |
|----------|----|----|----|-----|
| Q01 I am confident in building my own ML pipelines. | 1.85 | 4.10 | 4.00 | 2.96 |
| Q02 I am familiar with scikit-learn. | 2.08 | 3.70 | 4.33 | 2.96 |
| Q03 I am familiar with AutoML. | 1.77 | 2.20 | 4.67 | 2.27 |
| Q04 I understand how AutoML tools work. | 1.38 | 2.90 | 4.33 | 2.31 |
| Q05 I believe AutoML produces good models. | 2.46 | 3.30 | 3.67 | 2.92 |
Table 4. Table of all cards containing potential information presented during the card-sorting requirements analysis. Given is the mean rank of each card for domain experts (DE), data scientists (DS), AutoML researchers (AR), and all. A rank of 1 equals the most important information, a rank of 24 the least important.

| Task                                                                 | DE   | DS   | AR   | All  |
|----------------------------------------------------------------------|------|------|------|------|
| R01 View the input data                                             | 13.1 | 18.1 | 11.0 | 14.8 |
| R02 Know context information about features in the input data        | 7.9  | 14.9 | 16.0 | 11.5 |
| R03 View statistics of input data                                   | 10.3 | 19.3 | 14.0 | 14.2 |
| R04 Visualize the input data                                        | 11.3 | 17.1 | 17.7 | 14.3 |
| R05 View the pre-processed data                                     | 13.7 | 18.7 | 17.3 | 16.0 |
| R06 Know how input data was pre-processed                           | 15.4 | 11.3 | 15.7 | 13.8 |
| R07 View statistics of pre-processed data                           | 10.0 | 13.5 | 17.0 | 12.2 |
| R08 Visualize pre-processed data                                    | 13.2 | 14.0 | 22.0 | 14.5 |
| R09 View data after features engineering                            | 9.2  | 13.7 | 17.3 | 11.8 |
| R10 View statistics of data after feature-engineering               | 11.2 | 16.0 | 16.3 | 13.6 |
| R11 Visualize data after feature-engineering                        | 10.0 | 13.8 | 20.7 | 12.7 |
| R12 Know how new features are derived from existing features        | 11.8 | 10.2 | 16.3 | 11.7 |
| R13 View the complete processing pipeline                            | 16.2 | 6.7  | 10.7 | 11.9 |
| R14 Know which pre-processing, feature engineering, and modeling algorithms are available | 15.8 | 9.1  | 8.0  | 12.3 |
| R15 Know how pipelines are chosen                                   | 17.5 | 9.3  | 3.3  | 12.7 |
| R16 Know how hyperparameters are chosen                              | 17.8 | 13.9 | 5.0  | 14.8 |
| R17 View performance metrics                                        | 2.8  | 4.6  | 1.0  | 3.3  |
| R18 Visualize evaluation metrics                                    | 9.4  | 8.6  | 15.7 | 9.8  |
| R19 View global surrogates for model                                | 11.5 | 9.9  | 13.3 | 11.1 |
| R20 View local surrogates for model                                 | 9.5  | 8.4  | 13.0 | 9.5  |
| R21 View hyperparameters of model                                   | 17.7 | 15.1 | 8.7  | 15.7 |
| R22 Compare performance and explanations of various models with each other | 10.6 | 8.4  | 6.0  | 9.2  |
| R23 Compare pipeline structures with each other                     | 17.5 | 10.3 | 6.3  | 13.4 |
| R24 Compare hyperparameters of identical pipelines                  | 16.8 | 15.1 | 7.7  | 15.1 |

Table 5. Set of the tasks given to participants without expertise in ML with the percentage of correct answers.

| Task                                                                 | Correct % |
|----------------------------------------------------------------------|-----------|
| Optimization Overview                                                |           |
| T01 What performance does the best pipeline have?                    | 100       |
| T02 Is the best pipeline performing significantly better than the rest? | 100       |
| T03 Are better pipelines found over time?                            | 100       |
| T04 How many pipelines were generated in total?                      | 100       |
| Candidate Inspection                                                 |           |
| T11 What performance does the model have regarding <METRIC>?          | 100       |
| T12 Which rules does the model use for a prediction?                 | 100       |
| T13 What are the reasons for a single prediction?                    | 100       |
| T14 Which features are important?                                    | 100       |
Table 6. Set of the tasks given to participants with expertise in ML with the percentage of correct answers.

| Optimization Overview                              | Correct % |
|----------------------------------------------------|-----------|
| T21 What performance does the best pipeline have?  | 100       |
| T22 Is the best pipeline performing significantly better than the rest? | 100       |
| T23 Are better pipelines found over time?           | 94        |
| T24 How many pipelines were generated in total?     | 100       |

| Candidate Inspection                               | Correct % |
|----------------------------------------------------|-----------|
| T31 What steps does the pipeline have?              | 100       |
| T32 Which classifier does the pipeline use?         | 100       |
| T33 Which are the hyperparameters of this pipeline? | 94        |
| T34 How fast is a prediction using this pipeline?   | 100       |
| T35 Which are the most important hyperparameters?   | 100       |
| T36 What range should <HYPERPARAMETER> be to yield a good performance? | 94        |
| T37 Why was a single sample predicted as <CLASS>?    | 88        |
| T38 How does this pipeline approximately work?      | 100       |

| Search Space                                       | Correct % |
|----------------------------------------------------|-----------|
| T41 What does the search space look like?           | 94        |
| T42 Which classifier was most often used in all candidates? | 88        |
| T43 How many pipelines use an <ALGORITHM> as first step? | 94        |
| T44 How many hyperparameters does the random forest have? | 100       |
| T45 Does the search algorithm converge to a local minimum? | 94        |
| T46 Can you explain the how the search algorithm for pipelines works? | 94        |
| T47 Can you explain the how the search algorithm for hyperparameters works? | 94        |

| Ensemble Inspection                                | Correct % |
|----------------------------------------------------|-----------|
| T51 Which is the most important member in the ensemble? | 94        |
| T52 Are there models which should be removed from the ensemble? | 76        |