ABSTRACT

Automated Machine Learning (AutoML) systems are emerging that automatically search for possible solutions from a large space of possible kinds of models. Although fully automated machine learning is appropriate for many applications, users often have knowledge that supplements and constrains the available data and solutions. This paper proposes human-guided machine learning (HGML) as a hybrid approach where a user interacts with an AutoML system and tasks it to explore different problem settings that reflect the user’s knowledge about the data available. We present: 1) a task analysis of HGML that shows the tasks that a user would want to carry out, 2) a characterization of two scientific publications, one in neuroscience and one in political science, in terms of how the authors would search for solutions using an AutoML system, 3) requirements for HGML based on those characterizations, and 4) an assessment of existing AutoML systems in terms of those requirements.

CCS CONCEPTS

- Human-centered computing

KEYWORDS

Human-guided machine learning; Automated machine learning (AutoML); Task analysis; Scientific workflows.


1 Introduction

In recent years, Automated Machine Learning (AutoML) approaches are making great strides to automatically search for machine learning solutions from a large space of possible kinds of models. Typically, a solution is created by choosing a model (e.g., random forest, SVM, etc.) and then configuring those models by assigning (hyper)parameter values [1]–[4].

A series of challenges and workshops have led to steadfast improvements [5]. Commercial products are now becoming available that automate machine learning, notably for image classification and select natural language processing tasks [6]. While fully automated model learning is appropriate for many applications, there are many contexts where full automation is not desirable or possible.

This is the case when users have knowledge that supplements the available data, particularly in a scientific research context. An AutoML system would look at a set of instances or images the same whether they are about tumor tissues or ad placements. However, biologists would bring to bear extensive knowledge about human disease in the development of a machine learning model. Without this knowledge, machine learning models might optimize model search criteria but be inconsistent with what is known about the data and its context. Moreover, without incorporating this knowledge the solution search space might be intractable. In many cases, users explore alternative settings (different models, different features and different datasets) in order to consider a variety of questions and hypotheses.

This paper proposes human-guided machine learning (HGML) as a hybrid approach where a user interacts with an
AutoML system and tasks it to explore different problem settings that reflect the user’s knowledge about the data available. This requires an intelligent user interface that allows users to specify alternative problem settings and explore different models, and an AutoML system that can be tasked to generate solutions according to the user’s guidance. We explore requirements for HGML based on two substantial scientific publications in different disciplines (political science and neuroscience), and analyze how those requirements could be met by AutoML systems.

The main contributions of this paper are: 1) An integrated user interface and AutoML system that supports basic interactions as a baseline for HGML; 2) A task analysis of HGML that enumerates discrete user tasks to guide AutoML systems; 3) Characterizations of two significant studies in neuroscience and political science based on that task analysis; 4) Requirements for HGML resulting from those characterizations; and 5) An assessment of how those requirements could be accommodated by AutoML systems.

The paper begins with a description of an existing AutoML system that supports basic interactions with users. We then motivate why users could use their knowledge to effectively guide the search for machine learning models. We follow with a task analysis of common tasks involved in HGML, mapping these tasks to the steps followed in two recent publications in different disciplines. We then assess whether existing AutoML systems could accommodate those requirements. We finish with a discussion and an outline of future work.

2 Automating Machine Learning

A variety of approaches to AutoML have been explored in recent years. Auto-WEKA [1] combines automated model selection with (hyper)parameter optimization using the machine learning functions or primitives provided by the popular WEKA toolkit [7]. The approach was adopted for the scikit-learn library [8] in Auto-sklearn [2], extended with meta-learning and ensemble construction, and later with probabilistic matrix factorization [4]. TPOT offers an alternative approach using genetic algorithms [3].

3 Interacting with an AutoML System

In prior work, we integrated an AutoML system [10] with a user interface for statistical and machine learning model exploration [9] to allow users to specify machine learning problems of interest and have the AutoML system generate solutions. Figure 1 shows a snapshot of this system. The left-hand side summarizes the variables in a dataset, the middle portion highlights statistical properties of each variable (which can be explored further by the user), and the right-hand side shows how a user can specify a machine learning problem of interest. With that specification, the AutoML system returns the top ranked multi-step solutions that include an appropriate machine learning model.

Our AutoML system uses a phased approach to AutoML that can ingest naturally occurring data of any size and type, and use third-party data processing and modeling primitives [10]. In contrast with previous approaches to AutoML, this system can ingest different kinds of data such as tables, text, images and audio. The system exploits expert-like planning strategies to factor the search for multi-step solutions into phases: 1) extract features of interest from the dataset, 2) build a solution skeleton with the types of model and other steps to include, 3) address algorithm requirements with additional steps, 4) perform a hyperparameter search to improve the results, and 5) generate ensembles with the top-ranked models. The planner generates multi-step solutions that include featurization steps, data cleaning steps, imputation steps and modeling steps.

In this integrated system, a user specifies: 1) A target dataset with many instances (or data points); 2) A problem description (currently this can be classification or regression); 3) A specification of training and test data as subsets of the target dataset, including cross-validation details (number of folds, stratified or plain); and 4) An evaluation metric, which can be accuracy, mean squared error, and F1 macro. The system returns the top ranked solutions. Below are some example solutions for a classification problem to map questions to answers, showing the main steps and accuracy:
Towards Human-Guided Machine Learning

Our goal is to develop HGML systems that allow a domain expert, without a machine learning expert, to use relevant domain knowledge to inform the automated search for a high quality, impactful and interpretable model, including necessary data preparation steps necessary for analysis.

An HGML approach assumes iterative exploration and incremental development of models. That is, it does not assume a one-shot problem set up by the user and solution generation by the system. Users are expected to explore a variety of settings and models in order to understand the data and to formulate appropriate questions and hypotheses.

4 Human-Guided Machine Learning

We view human-guided machine learning (HGML) as a new area of research focused on how to assist users to use domain knowledge to guide an AutoML system to select machine learning algorithms and find multi-step solutions. Exploiting domain knowledge is particularly important for scientific data, which have been our focus to date.

There is important domain knowledge that can inform a predictive model but cannot be derived directly from a dataset or from abstract statistical or learning theory. This includes substantive theories about the context of the data, past results in the literature that lend prior weight to different factors and models, the purpose and properties of a good model, and the applicability of solutions from an AutoML system. This knowledge is complementary to the data itself.

In today’s very best research settings, where there are collaborations between domain experts and machine learning experts, exploration into the data is a joint venture where machine learning experts drive the computational machinery of analysis, but are directed to the interesting features by the knowledge of the domain experts. Often domain experts do not even realize what knowledge is most valuable, or what its implications are for tailoring the statistical choices, but a good machine learning collaborator can untangle and extract that information through discussion and model exploration. The goal of our work is to increasingly automate what a machine learning expert contributes to this process, so that a domain expert can develop machine learning models on their own.

Domain experts are typically heavily invested in the collection of their data, understand the variables well, pose questions that could be answered from the data, and possess substantive knowledge about the plausibility of various relationships that may emerge from models. What they may not know is the range of plausible models appropriate to their objectives, how to configure and parameterize models to explore the solution space, or how to interpret their results. We could imagine a hypothetical consulting machine learning expert whose role is to tease out all of the expert knowledge the researcher possesses, address any data quality issues, choose appropriate machine learning models, and then conduct tests as to whether the model has any failings. Alas, the extreme overabundance of data in many domains greatly surpasses the availability of such individuals, leaving many data-rich questions unresolved.

5 Related Work

The most closely related work is on interactive machine learning research and human-in-the-loop machine learning, a thorough review is provided in [11]. A variety of work has focused on interactive clustering, where users interact with a single type of clustering model, typically by requesting that clusters be split or merged. [16] focus on assisting a user to select parameter value ranges for clustering based on visualizations of a variety of metrics. In the case of clustering text data, there are approaches that allow users to provide additional kinds of input, such as term-based feedback on topic models [17]–[18]. Other work has focused on interactive feature selection for machine learning by developing user models based on prior interactions [19]. These approaches focus on helping a user set up and interact with machine learning models, while HGML allows users to task an AutoML system to do so.

Visual analytics focuses on approaches to generate visualizations that can help a user understand and analyze data, and even transform the data through manipulation [12]–[15]. Others have focused on exploring data through queries and statistic tests [20]–[21]. This exploration can lead a user to define new classes or features [22]. This work is complementary to HGML in that it focuses on helping users decide what features or classes to use rather than enabling them to specify features based on their knowledge.

There is also work on learning procedures from user logs or from demonstration [23]–[25], which could be the basis for HGML approaches that learn from watching users create end-to-end machine learning solutions in their domains.

In summary, prior work addresses issues of users providing input or reacting to a model generated by a machine learning algorithm, using the terms “interactive machine learning” or “human-in-the-loop machine learning”. There is no interaction on data preparation steps, which are known to affect the performance of machine learning models. There are also no choices of types models, as users interact with a single model (e.g., a k-means clustering model). In contrast, human-guided machine learning focuses on the user providing guidance to a fully automated machine learning system. Our work shifts the attention to maximizing machine learning automation, and takes...
### Task Category & Purpose

**Data Use**

**Variable Selection**

[VS1] The user may require that certain variables be given more priority

User’s domain knowledge indicates the importance of specific variables

Affect feature selection and weighting

[VS2] The user may suggest new variables that combine existing variables

User’s domain knowledge and experience indicates new variables

Affect feature generation

[VS3] The user may modify the framing (e.g., temporal, spatial) in which the variables exist

User is interested in a particular time period or area

Affect feature selection

[VS4] The user may fill in missing values in data based on existing variables

User’s domain knowledge indicates other variables may be good indicators

Affect missing value imputation

[VS5] The user may augment the available data with new variables

User may know of related data sources that can be brought to bear

Affect data and feature availability

**Variable Requirements**

[VR1] The user may ask that certain variables be included or excluded in a model

User’s domain knowledge indicates certain variables are good/bad predictors for the task at hand

Affect feature selection/filtering

**Data Generation**

**Instance Selection**

[IS1] The user may highlight instances that need to be accounted for in the model

The user is interested in target instances for the analysis at hand

Affect the instances used to train a model

[IS2] The user may select a subpopulation based on properties of the instances

User’s knowledge indicates sub-population may lead to more precise analysis

Affect the instances used to train a model

[IS3] The user may remove specific instances (e.g., outliers, poor quality, etc.)

The user believes that certain instances in the dataset will bias the model in undesirable ways

Affect the instances used to train a model

[IS4] The user selects training and test data, optionally with cross-validation specifications

The user may want to explore different training and test data splits of the data

Affect the instances used to train and test a model

**Model Development**

**Model Selection**

[MS1] The user may request a specific type of model

Users may have preferences (e.g., for a causal model or an explanatory model)

Affect the models included in the solution

[MS2] The user may request a specific type of model to replace the model in a prior solution

User question of interest may redefine what models are appropriate to the task at hand

Affect the models included in a solution

**Parameter Settings**

[PT1] The user may request the use of specific parameter values

User’s knowledge may indicate target parameters to reach a good solution efficiently

Configure models included in the solution

**Solution Design**

[SD1] The user may request specific data preparation steps (primitives or more general steps) to be present in the solution

User’s domain knowledge indicates that a certain feature generation or imputation step may be required

Affect the models included in the final solution

[SD2] The user may request to replace a data preparation step in a prior solution with a new step

User domain knowledge may assist search, or user may want to investigate consequences of model choices

Affect the models included in the final solution

**Model Interpretation**

**Model Assessment**

[QC1] The user may request quantities of interest to be computed

Users may request metrics, the regression slope, or ask for other means of interpreting a model

Perform computations on the data or model

[QC2] The user may request certain intermediate results that may be of interest

Intermediate results may indicate how a solution is analyzing data, and what features are being considered

Record intermediate results of the analysis

**Model Comparison**

[MC1] The user may ask for two or more solutions each with a different type of model

Users may want to compare alternatives (e.g., based on model performance or explainability)

Generate several solutions

[MC2] The user may ask for two or more solutions with a given model but each trained on different subsets of the instances

Users may want to compare how models differ when trained with different data

Generate several solutions

[MC3] The user may ask to compare two or more solutions with the same model but different data preparation steps

Users may want to find an explanation for the results provided to understand the different steps that appear in different solutions

Compare provenance records (i.e., steps, parameters, etc.) of two solutions

[MC4] The user may ask to compare two or more solutions with the same model but different parameters

User wants to understand the sensitivity of the model to different parameters

Compare provenance records of solutions

[MC5] The user may ask for a comparison between two models, all other solution steps being the same

Users may want an explanation of why two models have different performance

Generate a comparison of models

[MS2] The user may request a specific type of model

Users may have preferences (e.g., for a causal model or an explanatory model)

Affect the models included in the solution

**Parameter Comparison**

[PC1] The user may ask for several solutions, each with the same model or model primitive but a range of parameter values for one or more parameters

Users may want to validate a solution by verifying that is not significantly affected by a given parameter

Generate several solutions

Table 1. Major Tasks Involved in Human-Guided Machine Learning (HGML).
the user interactions further to collaborate with an AutoML system that can: 1) take on a variety of machine learning tasks on a wide range of types of data, 2) explore several model types, and 3) consider entire end-to-end solutions that include data preparation and feature generation steps.

6 Task Analysis

This section describes our task analysis work to characterize common tasks involved in human-guided machine learning. We followed two phases, the first was top-down and the second bottom up.

Table 1 summarizes the resulting tasks, showing in boldface the tasks that resulted from the second phase of the analysis.

We omit for brevity 2 tasks concerning hypothesis generation and testing, since they are not yet supported by existing AutoML systems. A detailed description of the tasks is available in [26].

6.1 First Phase: Initial Task Analysis

In the first phase, we took a top-down approach and articulated and categorized an initial set of tasks based on our understanding of how users work with machine learning algorithms to develop applications and our expectation of how they would want to interact with an AutoML framework. Table 1 shows the resulting 13 tasks (in light typestyle), grouped under general purpose and three major categories:

1. **Data Use:** Tasks concerning use of data allow users to specify which observations (rows) and features (columns) should be used to generate a machine learning model specific to the user’s foundational question of interest. For example, experts might need to remove data points that are not relevant to the question at hand, or give priority to observations that are more important to correctly predict. They might wish to include certain variables based on prior knowledge in the literature or to explicitly test a theory of interest, or remove variables they know cannot be related to increase the speed of the automated model search [27].

2. **Model Development:** Model development tasks broadly involve the user constraining the space of possible models beyond what could automatically be computed. Users may have prior knowledge or judgements they can provide that (directly or indirectly) help to tune model parameters. More importantly, the underlying purpose of their analysis, (which only they know) may change what models are appropriate. For example, in causal analysis there is a need for machine learning models that avoid bias [28].

3. **Model Interpretation:** Interpretation of machine learned models allows the user to guide how diagnostics and predictions from the model best illuminate the questions of interest the expert is interested in understanding. Also, directly comparing the performance of differently constructed models allows the researcher to better understand what the models infer about the world.

6.2 Second Phase: Annotation of Research Publications

In this phase, we followed a bottom-up approach and analyzed two very different publications where the authors describe a series of models, and annotated the author’s activities according to our tasks based on the author’s notes in the papers. That is, we tried to envision what the interaction would be between the article authors and an HGML system. This used the 13 tasks we had categorized, and added 10 more tasks shown in boldface in Table 1. A more detailed analysis is provided in [29].

6.2.1 Neuroscience Analysis. learning analysis produced by the ENIGMA neuroscience consortium [32]. ENIGMA aims to conduct large-scale collaborative research studies that show reliable and reproducible findings with greatly improved statistical power. The article analyzed here [30]-[31] aims to come to an unbiased consensus on the extent to which brain scans can classify patients with major depressive disorder (MDD) in the largest study of its kind.

Data for the consortium is pooled from independent MDD studies from around the world, allowing for a combined dataset of over 2,500 samples. Each individual study, or “cohort”, recruited both healthy individuals and patients with clinically diagnosed depression, and collected MRI and clinical data according to independent criteria (e.g., some were studies of younger adults, some older, some had no age restriction, some were more medicated, some were unmedicated, etc.; all were studies of MDD). While many classification attempts have shown over 80% accuracy in MDD classification from imaging measures (see [33] for an extensive review), most studies had been limited in power with less than 50 samples in each group and lacked independent replication in a separate sample. Furthermore, publication bias where null or unremarkable results are not published, has limited reports of more modest or unsuccessful classification attempts.

Table 2 gives an overview of our analysis of the article, showing the identifier for the user interaction, the task type corresponding to the tasks in Table 1, and a brief description. The authors explore 6 different models.

The authors choose one cohort in the list of cohorts as the test data and all the other cohorts as the training data. This is done to prevent data leakage, such that the test data was collected on a brain scanner that is different from those used in the training data, and had its own specifications on patient and control inclusion and exclusion criteria. In other words, the classification is performed to evaluate MDD diagnosis independent of specific study conditions. Leaving out an entire cohort for testing could reflect the actual performance of the models on unseen data collection.

After conducting the classification using the entire set of samples, the authors further refined their models to be trained and tested, or just tested, on a specific subset of samples determined by clinical, non-imaging related features. In Model 3, 4, 5, and 6 the classification was set according to factors such as the sex of the participants and whether the MDD patients had multiple
Table 2. Task Analysis for Neuroscience Article.

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>VR1</td>
<td>Leave out non-brain-image columns (&quot;sex&quot; and &quot;Episodes&quot;).</td>
</tr>
<tr>
<td>N2</td>
<td>IS2/VR1</td>
<td>Eliminate subjects whose age is over 21, and then drop the column &quot;age&quot;.</td>
</tr>
<tr>
<td>N3</td>
<td>IS3</td>
<td>Drop all rows with missing values.</td>
</tr>
<tr>
<td>N4</td>
<td>IS2</td>
<td>Set up training set as all cohorts (sites) but one, each time leaving out a cohort as test set.</td>
</tr>
<tr>
<td>N5</td>
<td>VR1</td>
<td>Drop columns &quot;subj&quot; and &quot;site&quot; from both training data and test data.</td>
</tr>
<tr>
<td>N6</td>
<td>IS4</td>
<td>Use stratified cross validation to evaluate the model trained on partial training set.</td>
</tr>
<tr>
<td>N7</td>
<td>MS1</td>
<td>Run Lasso on training set to gain feature importance (weights).</td>
</tr>
<tr>
<td>N8</td>
<td>VS1</td>
<td>Use the feature weights produced by Lasso and larger than 0 to select important features for modeling. If there are more than 5 features whose weights are large than 0, only keep the most important 5 features.</td>
</tr>
<tr>
<td>N9</td>
<td>MS1/PT1</td>
<td>Build a SVM model with specified parameters: kernel=rbf, gamma={1e-1, 1e-5}, c={1, 10, 100, 1000} for a grid search.</td>
</tr>
<tr>
<td>N10</td>
<td>QC1</td>
<td>Use multiple metrics (sensitvity, specificity, accuracy, balanced accuracy, F1 score, Matthews correlation coefficient and confusion matrix) to evaluate model performance. Accuracy, F1 score and Confusion Matrix are used to evaluate the model directly and other metrics are for comparison to previous publication.</td>
</tr>
<tr>
<td>N11</td>
<td>PD1</td>
<td>Perform N7 to N10 on the whole training set and use the test set to evaluate model performance.</td>
</tr>
</tbody>
</table>

**Model 2 (Logistic Regression with brain image features)**

- N1 – N6 same as above
- N12 | M5/P1T1 | Build Logistic Regression model with specified parameters, penalty=l1, solver=liblinear, class_weight=balanced. |
- N10 same as above
- N13 | PD1 | Perform N12 and N10 on the whole training set and use the test set to evaluate model performance. |

**Model 3 (Lasso + SVM with brain image features and splitting test set based on recurrence)**

- N2 – N10 same as above
- N16 | IS2 | Split all test instances into two groups by their "recur" values (1 and 2). Then the user can observe if there is a difference in predictions between the two groups of test data, which can show the influence of the "recur" feature to the model. |
- N11 same as above

**Model 4 (Logistic Regression with brain image features and splitting test set based on recurrence)**

- N14 | N15 and N2 – N6 and N12 and N10 and N16 and N13 same as above

**Model 5 (Lasso + SVM with brain image features and splitting test set based on sex)**

- N17 | VR1 | Leave out the non-brain-image column "sex". |
- N2 – N10 same as above
- N18 | IS2 | Split all test instances into two groups by their "sex" values (1 or 2). Then the user can observe if there is a difference in predictions between the two groups of test data, which can show the influence of the "sex" feature to the model. |
- N11 same as above

**Model 6 (Logistic Regression with brain image features and splitting test set based on sex)**

- N17 and N2 – N6 and N12 and N10 and N18 and N13 same as above

Depressive episodes. By comparing their performance, the generalizability and specificity of the models is exposed.

The authors did not include non-imaging features (i.e., age, sex) in models 1 and 2, but those features were included in models 3, 4, 5 and 6. While the imaging features were of primary interest, factors such as sex and age are related to the distribution of the imaging brain measures, so by comparing models 1 and 2 versus models 3, 4, 5, and 6, the authors could compare the performance of imaging measures alone to models that also account for basic patient demographic information, which would almost always be available in a clinical setting.

6.2.2 Political Science Analysis. In [34] Fearon provides a quintessential style of analysis in social science, which we call "empirical robustness." The author is interested in whether a hypothesis is supported across alternative data and modeling specifications. The hypothesis explored is that primary commodity exports (sxp) increase the likelihood of civil war onset. Earlier work by Collier and Hoeffler [35] argue sxp to be the primary driver of civil war risk. To demonstrate the fragility of their findings, Fearon first identifies points where Collier and Hoeffler chose one of several viable paths in model construction. For example, Collier and Hoeffler use a five-year data aggregation when a single-year aggregation is equally justifiable. He then shows that the empirical relationship between sxp and civil war onset is not robust under these alternative specifications.

While AutoML systems could take Fearon’s or Collier and Hoeffler’s data and produce a model to predict the onset of civil conflict, they would not be able to identify the policy relevance of sxp, the widespread impact of Collier and Hoeffler’s work, and thus the need to thoroughly assess the finding’s fragility. Furthermore, Fearon’s expertise with this type of data and his substantive knowledge of civil wars allowed him to identify a meaningful set of alternative viable paths. The domain knowledge that he brings to bear on this problem is outside, or auxiliary to, the data itself.

Table 3 shows the interaction tasks for each of the steps involved in creating all the models reported in Fearon’s article. He begins with a replication of Collier and Hoeffler’s base model (Step
Table 3. Task Analysis for Political Science Article.

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Type</th>
<th>Dataset</th>
<th>Description of Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon develops a logistic regression model with specified variables from Collier and Hoeffler’s dataset (DS1) and tests the joint significance of primary commodity exports (sxp) and exp^2 with a likelihood ratio test (χ^2 test).</td>
</tr>
<tr>
<td>F2</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon adds log(population) to the F2 model, resulting in sxp’s coefficient approaching the value in F1. He runs a χ^2 test, noticing the impact of sxp and log(population), with civil war onset probability at .11 in the 90th percentile of sxp.</td>
</tr>
<tr>
<td>F3</td>
<td>IS2</td>
<td>DS1</td>
<td>Fearon hypothesizes χ^2 test in F3 passed due to the impact of large countries, as they have low commodity exports as a percentage of GDP, but a higher civil war risk. He creates TABLE 3, which includes the proportion of civil war onset at the intersections of country population and exp trecilles.</td>
</tr>
<tr>
<td>F4</td>
<td>MS1</td>
<td>DS1</td>
<td>Fearon develops a logistic regression model with specified variables from Collier and Hoeffler’s dataset (DS1) and tests the joint significance of primary commodity exports (sxp) and exp^2 with a likelihood ratio test (χ^2 test).</td>
</tr>
<tr>
<td>F5</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon determines F1 feature significance by developing a logistic regression model using sxp and exp^2 and runs a χ^2 test. He notices a weak relationship, but unlikely due to chance.</td>
</tr>
<tr>
<td>F6</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon determines F1 feature significance by developing a logistic regression model using sxp and exp^2 and runs a χ^2 test. He notices a weak relationship, but unlikely due to chance.</td>
</tr>
<tr>
<td>F7</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon determines F1 feature significance by developing a logistic regression model using sxp and exp^2 and runs a χ^2 test. He notices a weak relationship, but unlikely due to chance.</td>
</tr>
<tr>
<td>F8</td>
<td>VR1, MS1, QC1</td>
<td>DS1</td>
<td>Fearon determines F1 feature significance by developing a logistic regression model using sxp and exp^2 and runs a χ^2 test. He notices a weak relationship, but unlikely due to chance.</td>
</tr>
<tr>
<td>F9</td>
<td>VR1, MS1, QC1</td>
<td>DS3</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from F8 and runs a χ^2 test.</td>
</tr>
<tr>
<td>F10</td>
<td>VR1, MS1, QC1</td>
<td>DS3</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from F8 and runs a χ^2 test.</td>
</tr>
<tr>
<td>F11</td>
<td>VR1, MS1, QC1</td>
<td>DS4</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F12</td>
<td>VR1, MS1, QC1</td>
<td>DS5</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F13</td>
<td>VR1, MS1, QC1</td>
<td>DS5</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F14</td>
<td>VR1, MS1, QC1</td>
<td>DS5</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F15</td>
<td>VR1, MS1, QC1</td>
<td>DS5</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F16</td>
<td>VR1, MS1, QC1</td>
<td>DS6</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F17</td>
<td>VR1, MS1, QC1</td>
<td>DS6</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F18</td>
<td>VR1, MS1, QC1</td>
<td>DS6</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F19</td>
<td>VR1, MS1, QC1</td>
<td>DS7</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F20</td>
<td>VR1, MS1, QC1</td>
<td>DS7</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F21</td>
<td>VR1, MS1, QC1</td>
<td>DS8</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F22</td>
<td>VR1, MS1, QC1</td>
<td>DS8</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F23</td>
<td>VR1, MS1, QC1</td>
<td>DS9</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F24</td>
<td>VR1, MS1, QC1</td>
<td>DS2</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F25</td>
<td>MS1</td>
<td>DS2</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F26</td>
<td>VR1</td>
<td>DS2</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
<tr>
<td>F27</td>
<td>MS1</td>
<td>DS2</td>
<td>Fearon drops fractionalization, ethnic dominance, and geographic dispersion from the logistic regression model. He runs a χ^2 test, noting lower statistical significance than TABLE 2 MODEL 6.</td>
</tr>
</tbody>
</table>

**Notes:**
- TABLE 2 MODEL 1 (Collier and Hoeffler Model Replication)
- TABLE 2 MODEL 2 (Adjusting from Parabolic to log Relationship)
- TABLE 2 MODEL 3 (Making Temporal Framing Adjustments)
- TABLE 2 MODEL 4 (Dropping Control Variables)
- TABLE 2 MODEL 5 (Filling Missing Data with Multiple Imputation)
- TABLE 2 MODEL 6 (Dropping Control Variables on Modified Dataset)
- TABLE 2 MODEL 7 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 3 MODEL 1 (Filling Missing Data with Multiple Imputation)
- TABLE 3 MODEL 2 (Dropping Control Variables on Modified Dataset)
- TABLE 3 MODEL 3 (Adjusting Temporal Frame on Modified Dataset)
- TABLE 3 MODEL 4 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 3 MODEL 5 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 3 MODEL 6 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 3 MODEL 7 (Hypothesis Testing Government Observance of Contracts)
- TABLE 4 MODEL 1, 2, and 3 (Dropping Control Variables with an adjusted log Relationship)
- TABLE 4 MODEL 4 (Dropping Control Variables with an adjusted log Relationship)
- TABLE 4 MODEL 5 (Dropping Control Variables with an adjusted log Relationship)
- TABLE 4 MODEL 6 (Dropping Control Variables with an adjusted log Relationship)
- TABLE 4 MODEL 7 (Dropping Control Variables with an adjusted log Relationship)
- TABLE 5 MODEL 1 (Filling Missing Data with Multiple Imputation)
- TABLE 5 MODEL 2 (Dropping Control Variables on Modified Dataset)
- TABLE 5 MODEL 3 (Adjusting Temporal Frame on Modified Dataset)
- TABLE 5 MODEL 4 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 5 MODEL 5 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 5 MODEL 6 (Dropping Control Variables from Temporally Modified Dataset)
- TABLE 5 MODEL 7 (Hypothesis Testing Government Observance of Contracts)
- TABLE 6 MODEL 1 (Collier and Hoeffler Model Replication)
- TABLE 6 MODEL 2 (Adjusting from Parabolic to log Relationship)
- TABLE 6 MODEL 3 (Making Temporal Framing Adjustments)
- TABLE 6 MODEL 4 (Dropping Control Variables)
- TABLE 6 MODEL 5 (Dropping Control Variables)
- TABLE 6 MODEL 6 (Dropping Control Variables)
- TABLE 6 MODEL 7 (Hypothesis Testing Government Observance of Contracts)
- TABLE 7 MODEL 1 (Hypothesis Testing Government Observance of Contracts)
- TABLE 7 MODEL 2 (Dropping Fuel Exports to Government Observance of Contracts)
- TABLE 8 MODEL 1 (Adding Fuel Exports to Government Observance of Contracts)

**References:**
- Fearon creates a regression model, with the estimated coefficient for sxp becoming statistically insignificant, but fuel exports maintaining significance. Oil exporters thus have weaker states given income per capita, and while exporters of other commodities have marginally less reliable governments on average, they are not consistently weak.
Here, $sxp$ and $sxp^2$ are each statistically significant, and a likelihood ratio test shows the pair is jointly significant. The same holds for a model containing only $sxp$ and $sxp^2$ as predictors ($F2$). He adds $\log(population)$ to this reduced model ($F3$) and shows comparably sized effects for $sxp$ and $sxp^2$ between this reduced model and the base model. He splits the data into trecileys by population and $sxp$/GDP to show that the core empirical finding is present only for large states. Then, Fearon explores a number of alternative viable modeling decisions to show the fragility of this base finding.

Briefly, he shows that $\log(sxp)$ is statistically significant ($F6$) and uses a generalized additive model to provide some empirical support for using $\log(sxp)$ instead of $sxp$ and $sxp^2$ ($F5$). He disaggregates the data from five-year to one-year observations ($F7$) and re-estimates the baseline model ($F8$), along with additional models containing $\log(sxp)$ and different sets of control variables ($F9$-$F11$). Fearon then uses multiple imputation for both the five-year and one-year datasets and re-estimates ($F12$-$F14$). In sum, the empirical relationship between primary commodity exports and civil war onset disappears, as evidenced in p-values for $sxp$, $sxp^2$, $\log(sxp)$, and the likelihood ratio tests for the joint significances of $sxp$ and $sxp^2$ across different models.

Through this process we have identified a number of core requirements for the empirical robustness feature. However, Fearon briefly touches upon alternative modeling decisions, particularly with human-guided modifications to the dataset, but chooses not to explore them further. One example involves the inconsistencies in attributing civil wars to countries; e.g., the separatist movement in Azerbaijan in 1964 (when it was part of the USSR) was coded as a civil war in Azerbaijan, while civil unrest in Chechnya in the 1990s (when it was part of the USSR and Russia) was coded as a civil war in Russia. Other inconsistencies appear in the many anti-colonial movements in the 1950s and 1960s that led to conflicts and independent nations across much of Asia and Africa, and in the 2000s in East Timor. Thus, a more thorough assessment of the finding’s empirical robustness would include datasets that identify civil conflicts using different criteria (e.g. [36]).

Similarly, Fearon notes trouble in collecting economic data at the time when Collier and Hoefler conducted their analysis, ensuring many states facing conflict were omitted from the dataset. With data now more accessible, additional conflicts can be tracked, even if the dataset is uniquely formatted. Methods can be developed to normalize the data sets in ways that ensure model compatibility.

6.2.3 Discussion. The analysis of the two articles confirmed that the tasks resulting from our top-down analysis do occur when users are developing machine learning models. The bottom-up analysis resulted in 10 additional tasks, shown in bold in Table 1: VS3, VS4, VS5, IS3, IS4, MS2, SD2, MC3, MC4, MC5. Although the two articles were selected for their diversity and their documentation of the exploration of solutions, other articles may uncover additional tasks.

We noticed that in both articles the researchers iterate over a very general pattern consisting of four stages:

A. There is first a set of tasks focused on feature selection and generation (Tasks VR1, VS2, VS3, IS2, IS3)
B. There is then a set of steps focused on selecting the model (Task MS1)
C. (Optionally) configuring the model with feature weights or parameter values (Tasks VS1, PT1)
D. There is then a request for quantities of interest and metrics (Task QC1)

The specifics of feature generation and selection vary very widely as the researchers explore different models.

Another significant observation is that there are a few tasks from our initial task analysis that did not come up in the analysis of these articles. Asking for intermediate results (QC2) did not appear in the narrative of the articles, but we are sure that the researchers did look at intermediate data. Imputation based on other variables (VS4) did not appear either, but we know this is a very common task and we expect at least the neuroscience researchers took a shortcut by removing values (IS3) instead. Augmenting the data (VS5) does not appear, but it is something that was pursued by other work in [36] mentioned earlier.

Perhaps the most interesting observation concerns how a user would build on previous solutions and models. Although the tasks that involve model and solution comparison (MC1-MC3) did not appear directly in the analysis of the articles, they are implicit in the task sequence. The neuroscience article was comparing SVM and logistic regression (MC1), using different populations (MC2), and using different features (MC3). The social sciences article leans more heavily on feature generation and selection (MC3).

Although this was not apparent in the articles analyzed, we expect that users would interact with an AutoML system by taking a previous solution and modifying it, or exploring variations of it. Therefore, we added comparison of model parameters and comparison of models (MC4-MC5). In addition, if users compare solutions or models, we would expect that they would request new solutions that are variations of previous ones. Hence, we added tasks for replacing models (MS2) and replacing data preparation steps (SD2) in prior solutions. HGML has the potential not only for bringing users the power of exploring additional machine learning models more efficiently, but allowing them to easily compare solutions in a more compact and effective manner.

7 Designing HGML Systems

Effective design of HGML systems require mapping the task analysis into requirements for the user interface and for the AutoML planner.

Table 4 summarizes user interface requirements (URe) and AutoML planner requirements (PRe) for HGML. Some tasks mapped to multiple requirements and some requirements spanning across multiple tasks.
## Table 4. Requirements for Human-Guided Machine Learning.

<table>
<thead>
<tr>
<th>Task</th>
<th>User Interface Requirements</th>
<th>Machine Learning Planner Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>[VS1] The user may require that certain variables be given more priority</td>
<td>URe1: Allow user to specify the priority of variables to be included in the model</td>
<td>PRe1: Planner must use modeling primitives that accept guidance about the relative weight of different variables</td>
</tr>
<tr>
<td>[VS2] The user may suggest new variables that combine existing variables</td>
<td>URe2: Allow user to select features to be combined and to create a specific rule or function to generate the new values</td>
<td>PRe2: Planner must add a feature generation primitive based on a user-provided rule or function</td>
</tr>
<tr>
<td>[VS3] The user may modify the framing (e.g., temporal, spatial) in which the variables exist</td>
<td>URe3: Allow user to create additional data points or eliminate data points from the dataset based on time and space qualifiers</td>
<td>(No requirement)</td>
</tr>
<tr>
<td>[VS4] The user may fill in missing values in data based on existing variables</td>
<td>URe4: Allow user to define a rule or function to generate the missing values</td>
<td>PRe4: Planner must perform an imputation step based on a user-provided rule or function</td>
</tr>
<tr>
<td>[VS5] The user may augment the available data with new variables</td>
<td>URe5: Allow user to merge new variables with existing data</td>
<td>(No requirement)</td>
</tr>
<tr>
<td>[VR1] The user may ask that certain variables be included or excluded in a model</td>
<td>URe6: Allow user to select variables to be included or excluded from the model</td>
<td>PRe5: Planner must use modeling primitives that accept guidance about what variables need to be included in the model</td>
</tr>
<tr>
<td>[IS1] The user may highlight instances that need to be accounted for in the model</td>
<td>URe7: Allow user to select instances that need to be accounted for in the model</td>
<td>PRe6: Planner must use modeling primitives that accept guidance about instances to be included in the model</td>
</tr>
<tr>
<td>[IS2] The user may select a subpopulation based on properties of the instances</td>
<td>URe8: Allow user to specify parameters indicative of a subpopulation to divide the data</td>
<td>(No requirement)</td>
</tr>
<tr>
<td>[IS3] The user may remove specific instances (e.g., outliers, poor quality, etc)</td>
<td>URe10: Allow user to remove instances from dataset</td>
<td>(No requirement)</td>
</tr>
<tr>
<td>[IS4] The user selects training and test data, optionally with cross-validation specifications</td>
<td>URe11: Allow user to group dataset instances into different combinations of training and test data</td>
<td>PRe7: Planner must accept a specification of training and test data and cross-validation requirements</td>
</tr>
<tr>
<td>[MS1] The user may request a specific type of model</td>
<td>URe12: Allow user to specify the class of model desired</td>
<td>PRe8: Planner should use a hierarchy of primitives grouped according to model type, and include the user selected class in the solution</td>
</tr>
<tr>
<td>[MS2] The user may request a specific type of model to replace the model in a prior solution</td>
<td>URe13: Allow user to select a previous solution and indicate what new model is desired</td>
<td>PRe9: Planner should modify a prior solution to include the new model</td>
</tr>
<tr>
<td>[FT1] The user may request the use of specific parameter values</td>
<td>URe14: Allow user to specify a model and the parameter values desired</td>
<td>PRe10: Planner should include user specified model and parameter values in the solution</td>
</tr>
<tr>
<td>[SD1] The user may request specific data preparation steps (primitives or more general steps) to be present in the solution</td>
<td>URe15: Allow user to specify types of data preparation primitives to be included in a solution (i.e. data imputation)</td>
<td>PRe11: Planner should include a hierarchy of primitives grouped by classes according to their function, and include the user selected class in the solution</td>
</tr>
<tr>
<td>[QC1] The user may request quantities of interest (QI’s) to be computed</td>
<td>URe16: Allow user to request a particular statistic test and parameters</td>
<td>PRe12: Planner should include primitives to generate metrics and standard statistical tests for models</td>
</tr>
<tr>
<td>[QC2] The user may specify certain intermediate results that may be of interest</td>
<td>URe17: Allow user to request results after any step in a solution</td>
<td>PRe13: Planner should return intermediate results of a pipeline</td>
</tr>
<tr>
<td>[MC1] The user may ask for two or more solutions each with a different type of model</td>
<td>URe18: Allow user to specify multiple models to be included in solutions that have otherwise the same steps</td>
<td>PRe7: (same as above)</td>
</tr>
<tr>
<td>[MC2] The user may ask for two or more solutions with a given model but each trained on different subsets of the instances</td>
<td>URe11 (same as above)</td>
<td>PRe14: Planner should generate solutions that use the same steps but differ in the type of model used</td>
</tr>
<tr>
<td>[MC3] The user may ask to compare two or more solutions with the same model but different data preparation steps</td>
<td>URe12 (same as above)</td>
<td>PRe6 (same as above)</td>
</tr>
<tr>
<td>[MC4] The user may ask to compare two or more solutions with the same model but different data preparation steps</td>
<td>PRe7 (same as above)</td>
<td></td>
</tr>
<tr>
<td>[MC5] The user may ask for a comparison between two models, all other solution steps being the same</td>
<td>URe19: Generate comparative explanations for two given solutions</td>
<td>PRe15: Planner must be able to return detailed provenance records of the solutions</td>
</tr>
<tr>
<td>[MC6] The user may ask for a comparison between two models, all other solution steps being the same</td>
<td>PRe16: Primitives must support explanation</td>
<td></td>
</tr>
<tr>
<td>[MC7] The user may ask for a comparison between two models, all other solution steps being the same</td>
<td>URe20: Contrast two solutions in terms of the steps involved</td>
<td>PRe15 (same as above)</td>
</tr>
</tbody>
</table>

---

**User Interface Requirements**

- **URe1**: Allow user to specify the priority of variables to be included in the model.
- **URe2**: Allow user to select features to be combined and to create a specific rule or function to generate the new values.
- **URe3**: Allow user to create additional data points or eliminate data points from the dataset based on time and space qualifiers.
- **URe4**: Allow user to define a rule or function to generate the missing values.
- **URe5**: Allow user to merge new variables with existing data.
- **URe6**: Allow user to select variables to be included or excluded from the model.
- **URe7**: Allow user to select instances that need to be accounted for in the model.
- **URe8**: Allow user to specify parameters indicative of a subpopulation to divide the data.
- **URe9**: Allow user to define a rule or function to generate a subpopulation.
- **URe10**: Allow user to remove instances from dataset.
- **URe11**: Allow user to group dataset instances into different combinations of training and test data.
- **URe12**: Allow user to specify the class of model desired.
- **URe13**: Allow user to select a previous solution and indicate what new model is desired.
- **URe14**: Allow user to specify a model and the parameter values desired.
- **URe15**: Allow user to specify types of data preparation primitives to be included in a solution (i.e. data imputation).
- **URe16**: Allow user to request a particular statistic test and parameters.
- **URe17**: Allow user to request results after any step in a solution.
- **URe18**: Allow user to specify multiple models to be included in solutions that have otherwise the same steps.
- **URe19**: Generate comparative explanations for two given solutions.
- **URe20**: Contrast two solutions in terms of the steps involved.

**Machine Learning Planner Requirements**

- **PRe1**: Planner must use modeling primitives that accept guidance about the relative weight of different variables.
- **PRe2**: Planner must add a feature generation primitive based on a user-provided rule or function.
- **PRe3**: Planner must include user specified primitives in the solution.
- **PRe4**: Planner must perform an imputation step based on a user-provided rule or function.
- **PRe5**: Planner must use modeling primitives that accept guidance about what variables need to be included in the model.
- **PRe6**: Planner must use modeling primitives that accept guidance about instances to be included in the model.
- **PRe7**: Planner must accept a specification of training and test data and cross-validation requirements.
- **PRe8**: Planner should use a hierarchy of primitives grouped according to model type, and include the user selected class in the solution.
- **PRe9**: Planner should modify a prior solution to include the new model.
- **PRe10**: Planner should include user specified model and parameter values in the solution.
- **PRe11**: Planner should include a hierarchy of primitives grouped by classes according to their function, and include the user selected class in the solution.
- **PRe12**: Planner should include primitives to generate metrics and standard statistical tests for models.
- **PRe13**: Planner should return intermediate results of a pipeline.
- **PRe14**: Planner should generate solutions that use the same steps but differ in the type of model used.
- **PRe15**: Planner must be able to return detailed provenance records of the solutions.
- **PRe16**: Primitives must support explanation.
7.1 Accommodating HGML User Interface Requirements

In our baseline system, described earlier, the focus is primarily on the construction of a solution, which entails a single interaction with the user and a single, known endpoint: a solution that includes an estimated model. In HGML, the interaction is no longer linear, as we extract domain knowledge before the model is constructed, we increase the number of models constructed and the user views those models and contributes more domain knowledge. Rather, the interaction is better characterized as iterative and nonlinear. It is iterative because models are returned, refined, and then re-estimated. It is nonlinear because a user may return to an earlier model, or go back to any associated options, after running an arbitrarily number of models with many different options selected.

Individually, the HGML requirements listed in Table 4 can be easily incorporated into our existing user interface. For example, formula builders and query constructors could be added to create new variables from existing ones (URe2) and to select subpopulations (URe7, URe8). These types of interactions may be facilitated with graphical displays of the data, for example brushable density plots.

More challenging will be the combination of HGML requirements to reflect the iterative and nonlinear nature of the interactions discussed above. For example, the user would need to refer to specific solutions and their individual steps in relation to one another (URe13-URe17). Data may be manipulated for one model, and that manipulation may be undone for the next, only to be recalled later in the session (URe13). Users may want to compare two solutions (URe17) where one step differs (URe16). Maintaining usability and transparency, essential for user trust, becomes more complex in such interactions.

7.2 Accommodating HGML Planner Requirements

Some requirements for the planner concern the primitives available to the planner for composing solutions. For modeling primitives, these would be to accept input about feature weights (PRe1), variables to be included in the model (PRe5), instances to be accounted for in the model (PRe6), and support explanation (PRe16). The planner would need to access metadata about primitives that describes them in this light. Our planner includes a metadata catalog that is extensible to new primitive metadata. The planner would have to be extended to accept constraints that restrict the solutions it generates accordingly. Other AutoML systems, such as AutoWEKA, Auto-sklearn, and TPOT, do not have metadata in their primitives, and would have to be extended in that way. The inclusion of primitives for generation of metrics and quantities of interest (PRe12) is not difficult to accommodate, as it simply involves having the primitives.

We note that when a user defines a feature generation step (PRe2) or imputation step (PRe4) this needs to be turned into a primitive that the planner incorporates into the solution, since it would have to be applied to the test data. Our planner does not yet support this, and neither do other planners. All consider the primitive library as pre-existing.

Another set of requirements concern seeding the solutions with some partial specification, so the search is restricted to solutions which conform to that specification. These requirements include the appearance of a certain imputation (PRe4) or data preparation primitive in the solution (PRe3), the use of a certain type of model (PRe8, PRe10, PRe11), and the use of specific parameter values for models (PRe10). Our planner has a phase where it builds a solution skeleton that it elaborates in later phases. It would have to be extended to accept a skeleton formed with the user’s requirements, which would not be very difficult. For AutoWEKA and Auto-sklearn, it would be relatively easy to support the use of a certain type of model, but not other requirements as they do not assemble multi-step solutions. For TPOT, which uses a genetic algorithm, it is unclear that the exploration for solutions could be controlled not to deviate from the initial skeleton.

Recording the provenance of the solutions generated would support important aspects of explanation and comparisons (PRe13 and PRe14). Our planner fully supports these.

Supporting the specification of training and test data and cross validation (PRe7) is an overarching function for solution generation. Our planner already supports this. Other planners would have to be extended accordingly.

Perhaps the most interesting extension stems from requirements about the use of a hierarchy of primitives grouped in classes (PRe8, PRe11). This would support users stating the increasingly more specific requests, for example, for “a naive Bayes classifier”, “a hierarchical Bayes classifier”, and the “sklearn-hierarchicalClassification primitive”. Our planner supports these hierarchies in its primitive catalog, both based on algorithm type (e.g., Bayesian vs deep learning primitives) and algorithm function (e.g., imputation vs feature generation primitives). Other AutoML planners do not currently support these hierarchies.

8 Conclusions

In this paper we presented requirements for human-guided machine learning, where domain experts use their knowledge to affect how an automated machine learning system generates models. These requirements are based on a task analysis of the different kind of interactions that would need to be supported between users and AutoML systems. We presented an analysis that reconstructs the potential interactions with such a system by the authors of two articles in neuroscience and social sciences that explore a variety of models. Our results show that users would follow repetitive patterns in their interactions. We also presented a baseline system that enables users to simply ask an AutoML system to generate a solution, and analyzed several AutoML systems in terms of how they would need to be extended to support the requirements. In future work, we plan to extend our baseline system with the requirements described in this paper. This would open exciting possibilities for domain experts to
Towards Human-Guided Machine Learning

generate machine learning models of improved quality for many problems without the help of machine learning experts.

ACKNOWLEDGMENTS

This material is based on research sponsored by the Defense Advanced Research Projects Agency (DARPA) under agreement numbers FA8750-17-C-0106 and FA8750-17-2-0114. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

REFERENCES


