

Automated Data Slicing for Model Validation: A Big Data - AI Integration Approach

Yeounoh Chung¹, Tim Kraska, Neoklis Polyzotis², Ki Hyun Tae³,
and Steven Euijong Whang⁴, *Senior Member, IEEE*

Abstract—As machine learning systems become democratized, it becomes increasingly important to help users easily debug their models. However, current data tools are still primitive when it comes to helping users trace model performance problems all the way to the data. We focus on the particular problem of slicing data to identify subsets of the validation data where the model performs poorly. This is an important problem in model validation because the overall model performance can fail to reflect that of the smaller subsets, and slicing allows users to analyze the model performance on a more granular-level. Unlike general techniques (e.g., clustering) that can find arbitrary slices, our goal is to find interpretable slices (which are easier to take action compared to arbitrary subsets) that are problematic and large. We propose SliceFinder, which is an interactive framework for identifying such slices using statistical techniques. Applications include diagnosing model fairness and fraud detection, where identifying slices that are interpretable to humans is crucial. This research is part of a larger trend of Big data and Artificial Intelligence (AI) integration and opens many opportunities for new research.

Index Terms—Data slicing, model validation, model analysis

1 INTRODUCTION

MACHINE learning systems [1] are becoming more prevalent thanks to a vast number of success stories. However, the data tools for interpreting and debugging models have not caught up yet, and many important challenges exist to improve our model understanding after training [2]. One such key problem is to understand if a model performs poorly on certain parts of the data, hereafter referred to as a *slice*.

Example 1. Consider a Random Forest classifier that predicts whether a person's income is above or below \$50,000 (UCI Census data [3]). Looking at Table 1, the overall metrics may be considered acceptable, since the overall log loss (a widely-used loss metric for binary classification problem) is low for all the data (see the "All" row). However, the individual slices tell a different story. When slicing data by gender, the model is more accurate for **Female** than **Male** (the *effect size* defined in Section 2 captures this relation by measuring the normalized loss metric difference between the **Male** slice and its counterpart, the **Female** slice). The **Prof-specialty** slice is interesting because the average loss metric is on par with **Male**, but the effect size is much smaller. A small effect size means that the loss metric on **Prof-specialty** is similar to the loss metric on other

demographics (defined as *counterparts* in Section 2). Hence, if the log loss of a slice and that of the counterpart are not acceptable, then it is likely that the model is bad overall, not just on a particular subset. Lastly, we see that people with higher education degrees (**Bachelors** < **Masters** < **Doctorate**) suffer from worse model performance, and their losses are higher than their counterparts and thus have higher error concentration. Thus, slices with high effect size are important for model validation, to make sure that the model does not underperform on certain parts of the data.

The problem is that the overall model performance can fail to reflect that of smaller data slices. Thus, it is important that the performance of a model is analyzed on a more granular level. While a well-known problem [4], current techniques to determine underperforming slices largely rely on domain experts to define important subpopulations (or at least specify a feature dimension to slice by) [5], [6]. Unfortunately, machine learning practitioners do not necessarily have the domain expertise to know all important underperforming slices in advance, even after spending a significant amount of time exploring the data. An underlying assumption here is that the dataset is large to the extent that enumerating all possible data slices and validating model performance for each is not practical due to the sheer number of possible slices. Worse yet, simply searching for the most underperforming slices can be misleading because the model performance on smaller slices can be noisy, and without any safeguard, this leads to slices that are too small for meaningful impact on the model quality or that are false discoveries (i.e., non-problematic slices appearing as problematic). Ideally, we want to identify the largest and true problematic slices from the smaller slices that are not fully reflected on by the overall model performance metric.

- Y. Chung is with Apple Inc, Cupertino, CA 95014. E-mail: yeounoh_chung@brown.edu.
- T. Kraska is with MIT, Cambridge, MA 02139. E-mail: kraska@mit.edu.
- N. Polyzotis is with Google Research, 1600 Amphitheatre Parkway, Mountain View, CA 94043. E-mail: npolyzotis@google.com.
- K. Tae and S.E. Whang are with KAIST, Daejeon 34141, Republic of Korea. E-mail: {kihyun.tae, swhang}@kaist.ac.kr.

Manuscript received 5 Jan. 2019; accepted 22 Apr. 2019. Date of publication 14 May 2019; date of current version 5 Nov. 2020.

(Corresponding author: Steven Euijong Whang.)

Recommended for acceptance by F. Rusu.

Digital Object Identifier no. 10.1109/TKDE.2019.2916074

TABLE 1
UCI Census Data Slices for Example 1

Slice	Log Loss	Size	Effect Size
All	0.35	30k	n/a
Sex = Male	0.41	20k	0.28
Sex = Female	0.22	10k	-0.29
Occupation = Prof-specialty	0.45	4k	0.18
Education = HS-grad	0.33	9.8k	-0.05
Education = Bachelors	0.44	5k	0.17
Education = Masters	0.49	1.6k	0.23
Education = Doctorate	0.56	0.4k	0.33

There are more generic clustering-based algorithms in model understanding [7], [8], [9] that group similar examples together as clusters and analyze model behavior locally within each cluster. Similarly, we can cluster similar examples and treat each cluster as an arbitrary data slice; if a model underperforms on any of the slices, then the user can analyze the examples within. However, clusters of similar examples can still have high variance and high cardinality of feature values, which are hard to summarize and interpret. In comparison, a data slice with a few common feature values (e.g., the Female slice contains all examples with Sex = Female) is much easier to interpret. In practice, validating and reporting model performance on interpretable slices are much more useful than validating on arbitrary non-interpretable slices (e.g., a cluster of similar examples with mixed properties).

A good technique to detect problematic slices for model validation thus needs to find easy-to-understand subsets of data and ensure that the model performance on the subsets is meaningful and not attributed to chance. Each problematic slice should be immediately understandable to a human. The problematic slices should also be large enough so that their impact on the overall model quality is non-negligible. Since the model may have a high variance in its prediction quality, we also need to be careful not to choose slices that are false discoveries. Finally, since the slices have an exponentially large search space, it is infeasible to manually go through each slice. Instead, we would like to guide the user to a handful of slices that satisfy the conditions above. In this paper we propose SliceFinder, which efficiently discovers large possibly-overlapping slices that are both interpretable and problematic.

A slice is defined as a conjunction of feature-value pairs where having fewer pairs is considered more interpretable. A problematic slice is identified based on testing of a significant difference of model performance metrics (e.g., loss function) of the slice and its counterpart. That is, we treat each problematic slice as a hypothesis and check that the difference is statistically significant, and the magnitude of the difference is large enough according to the effect size. We discuss the details in Section 2. One problem with performing many statistical tests (due to a large number of candidate slices) is an increased number of false positives. This is what is also known as Multiple Comparisons Problem (MCP) [10]: imagine a test of Type-I error (false positive: recommending a non-problematic slice as problematic) rate of 0.05 (a common α -level for statistical significance testing); the probability of having any false positives blows up exponentially with

the number of comparisons (e.g., $1 - (1 - 0.05)^8 = 0.34$, even for just 8 tests, but then, we may end up exploring hundreds and thousands of slices even for a modest number of examples). We address this issue in Section 3.2.

In addition to testing, the slices found by SliceFinder can be used to evaluate model fairness or in applications such as fraud detection, business analytics, and anomaly detection, to name a few. While there are many definitions for fairness, a common one is that a model performs poorly (e.g., lower accuracy) on certain sensitive features (which define the slices), but not on others. Fraud detection also involves identifying classes of activities where a model is not performing as well as it previously did. For example, some fraudsters may have gamed the system with unauthorized transactions. In business analytics, finding the most promising marketing cohorts can be viewed as a data slicing problem. Although SliceFinder evaluates each slice based on its losses on a model, we can also generalize the data slicing problem where we assume a general scoring function to assess the significance of a slice. For example, data validation is the process of identifying training or validation examples that contain errors (e.g., values are out of range, features are missing, and so on). By scoring each slice based on the number or type of errors it contains, we can summarize the data errors through a few interpretable slices rather than showing users an exhaustive list of all erroneous examples.

The main contribution of this paper is applying data management techniques to the model validation problem in machine learning. This application is part of a larger integration of the areas of Big data and Artificial Intelligence (AI) where data management plays a role in almost all aspects of machine learning [11], [12]. This paper extends our previous work on SliceFinder [13], [14]. In particular, we provide a full description of the slice finding algorithms and provide extensive experiments.

In summary, we make the following contributions:

- We define the data slicing problem and the use of hypothesis testing for problematic slice identification (Section 2) and false discovery control (Section 3.2).
- We describe the SliceFinder system and propose three automated data slicing approaches, including a naive clustering-based approach as a baseline for automated data slicing (Section 3).
- We present model fairness as a potential use case for SliceFinder (Section 4).
- We evaluate the automated data slicing approaches using real and synthetic datasets (Section 5).

2 DATA SLICING PROBLEM

2.1 Preliminaries

We assume a dataset D with n examples and a model h that needs to be tested. Following common practice, we assume that each example $x_F^{(i)}$ contains features $F = \{F_1, F_2, \dots, F_m\}$ where each feature F_j (e.g., country) has a list of values (e.g., {US, DE}) or discretized numeric value ranges (e.g., $[0, 50]$, $[50, 100]$). We also have a ground truth label $y^{(i)}$ for each example, such that $D = \{(x_F^{(1)}, y^{(1)}), (x_F^{(2)}, y^{(2)}), \dots, (x_F^{(n)}, y^{(n)})\}$. The test model h is an arbitrary function that maps an input example to a prediction using F , and the goal is to validate if

h is working properly for different subsets of the data. For ease of exposition, we focus on a binary classification problem (e.g., UCI Census income classification) with h that takes an example $x_F^{(i)}$ and outputs a prediction $h(x_F^{(i)})$ of the true label $y^{(i)} \in \{0, 1\}$ (e.g., a person's income is above or below \$50,000). Without loss of generality, we assume that the model uses all the features in F for classification.

A slice S is a subset of examples in D with common features and can be described as a predicate that is a conjunction of literals $\bigwedge_j F_j \text{ op } v_j$. The F_j 's are distinct (e.g., $\text{country} = \text{DE} \wedge \text{gender} = \text{Male}$) and form a subset of F . Each op can be one of $=, \neq, <, \leq, \geq, >$. For numeric features, we can discretize their values (e.g., quantiles or equi-height bins) and generate ranges so that they are effectively categorical features (e.g., $\text{age} = [20, 30)$). Numeric features with large domains tend to have fewer examples per value, and hence do not appear as significant. By discretizing numeric features into a set of continuous ranges, we can effectively avoid searching through tiny slices of minimal impact on model quality and group them to more sizable and meaningful slices.

We also assume a classification loss function $\psi(S, h)$ that returns a performance score for a set of examples by comparing h 's prediction $h(x_F^{(i)})$ with the true label $y^{(i)}$. A common classification loss function is logarithmic loss (*log loss*), which in case of binary classification is defined as:

$$-\frac{1}{n} \sum_{(x_F^{(i)}, y^{(i)}) \in S} [y^{(i)} \ln h(x_F^{(i)}) + (1 - y^{(i)}) \ln (1 - h(x_F^{(i)}))].$$

The log loss is non-negative and grows with the number of classification errors. A perfect classifier h would have log loss of zero, and a random-guesser ($h(x) = 0.5$) log loss of $-\ln(0.5) = 0.693$. Also note that our techniques and the problem setup can easily generalize to other machine learning problem types (e.g., multi-class classification, regression, etc.) with proper loss functions/performance metrics.

2.2 Model Validation

We consider the model validation scenario of pointing the user to "problematic" slices where a single model performs relatively poorly on. That is, we would like to find slices where the loss function returns a significantly higher loss than the rest of the examples in D . At the same time, we prefer these slices to be large as well. For example, the slice $\text{country} = \text{DE}$ may be too large for a model to perform significantly worse than other countries. On the other hand, the slice $\text{country} = \text{DE} \wedge \text{gender} = \text{Male} \wedge \text{age} = 30$ may have a high loss, but may also be too specific and thus small to have much impact on the overall performance of the model. Finally, we would like the slices to be interpretable in the sense that they can be expressed with a few literals. For example, $\text{country} = \text{DE}$ is more interpretable than $\text{country} = \text{DE} \wedge \text{age} = 20 - 40 \wedge \text{zip} = 12345$.

Finding the most problematic slices is challenging because it requires a balance between how significant the difference in loss is and how large the slice is. Simply finding a slice with many classification errors will not work because there may also be many correct classifications within the same slice (recall that a slice is always of the form $\bigwedge_j F_j \text{ op } v_j$). Another

solution would be to score each slice based on some weighted sum of its size and difference in average losses. However, this weighting function is hard to tune by the user because it is not clear how size relates to loss. Instead, we envision the user to either fix the significance or size.

2.3 Problematic Slice as Hypothesis

We now discuss what we mean by significance in more detail. For each slice S , we define its counterpart S' as $D - S$, which is the rest of the examples. We then compute the relative loss as the difference $\psi(S, h) - \psi(S', h)$. Without loss of generality, we only look for positive differences where the loss of S is higher than that of S' .

A key question is how to determine if a slice S has a significantly higher loss than S' . Our solution is to treat each slice as a hypothesis and perform two tests: determine if the difference in loss is statistically significant and if the effect size [15] of the difference is large enough. Using both tests is a common practice [15] and necessary because statistical significance measures the existence of an effect (i.e., the slice indeed has a higher loss than its counterpart) while the effect size complements statistical significance by measuring the magnitude of the effect (i.e., how large the difference is).

To measure the statistical significance, we use the hypothesis testing with the following null (H_o) and alternative (H_a) hypotheses:

$$\begin{aligned} H_o : \psi(S, h) &\leq \psi(S', h) \\ H_a : \psi(S, h) &> \psi(S', h). \end{aligned}$$

Here both S and S' should be viewed as samples of all the possible examples in the world, including the training data and even the examples that the model might serve in the future. We then use Welch's t -test [16], which is used to test the hypothesis that two populations have equal means and is defined as follows:

$$t = \frac{\mu_S - \mu_{S'}}{\sqrt{\sigma_S^2/|S| + \sigma_{S'}^2/|S'|}},$$

where μ_S is the average loss of S , σ_S is the variance of the individual example losses in S , and $|S|$ is the size of S . In comparison to Student's t -test, Welch's t -test is more reliable when the two samples have unequal variances and unequal sample sizes, which fits our setting. The p -value, which denotes the probability of finding an outcome at least as extreme as the one from the data when the null hypothesis is true, can be calculated from t -test. If the p -value is less than or equal to given significance level α (conventionally, α is set to 0.01 or 0.05 [17]), the hypothesis is rejected and regarded as statistically significant.

To measure the magnitude of the difference between the distributions of losses of S and S' , we compute the effect size [15] ϕ , which is defined as follows:

$$\phi = \sqrt{2} \times \frac{\psi(S, h) - \psi(S', h)}{\sqrt{\sigma_S^2 + \sigma_{S'}^2}}.$$

Intuitively, if the effect size is 1.0, we know that the two distributions differ by one standard deviation. According to

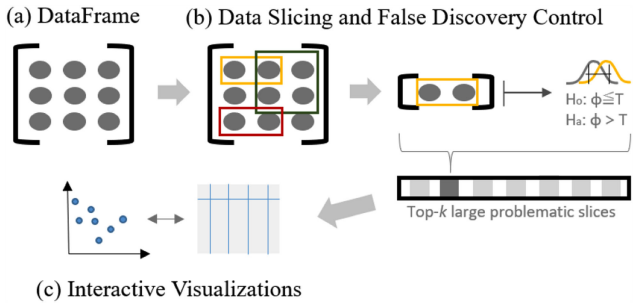


Fig. 1. The SliceFinder architecture: (a) Data is loaded into a Pandas DataFrame, (b) SliceFinder performs automated data slicing and false discovery control to find the top- k large problematic slices, and (c) SliceFinder provides interactive visualizations.

Cohen's rule of thumb [18], an effect size of 0.2 is considered small, 0.5 is medium, 0.8 is large, and 1.3 is very large.

2.4 Problem Definition

For two slices S and S' , we say that $S \prec S'$ if S precedes S' when ordering the slices by increasing number of literals, decreasing slice size, and decreasing effect size. For slices that have the same three values, we allow them to be ordered arbitrarily. In a sense, we are using an order-by semantics with multiple attributes. Then the goal of SliceFinder is to identify *problematic slices* as follows:

Definition 1. Given a positive integer k , an effect size threshold T , and a significance level α , find the top- k slices sorted by the ordering \prec such that:

- Each slice S has an effect size at least T ,
- The slice is statistically significant,
- No slice can be replaced with one that has a strict subset of literals and satisfies the above two conditions.

The top- k slices do not have to be distinct, e.g., `country = DE` and `education = Bachelors` overlap in the demographic of Germany with a Bachelors degree. In a user's point of view, setting the effect size threshold T may be challenging, so SliceFinder provides a slider for T that can be used to explore slices with different degrees of problematicness (see Section 3.3).

3 SYSTEM ARCHITECTURE

Underlying the SliceFinder system is an extensible architecture (Fig. 1) that combines automated data slicing and interactive visualization tools. SliceFinder loads the validation data set into a Pandas DataFrame [19]. The DataFrame supports indexing individual examples, and each data slice keeps a subset of indices instead of a copy of the actual data examples. SliceFinder provides basic slice operators (e.g., intersect) based on the indices; only when evaluating the machine learning model on a given slice does SliceFinder access the actual data by the indices to test the model. The Pandas library also provides a number of options to deal with dirty data and missing values. For example, one can drop *NAs* (missing values) or any values that deviate from the column types as necessary.

Once the data is loaded into a DataFrame, SliceFinder processes it to identify the problematic slices and allows the user

to explore them. SliceFinder searches for problematic slices either by training a CART decision tree around misclassified examples or by performing a more exhaustive search on a lattice of slices. Both search strategies progress in a top-down manner until they find the top- k problematic slices. The decision tree approach materializes the tree model and traverses the tree to find problematic slices. In lattice searching, SliceFinder traverses a lattice of slices to find the slices. This top-down approach allows SliceFinder to quickly respond to new request queries that use different k , as described in Section 3.3. As SliceFinder searches through a large number of slices, some slices might appear problematic by chance (i.e., multiple comparisons problem [20]). SliceFinder controls such a risk by applying a marginal false discovery rate (mFDR) controlling procedure called α -investing [17], [20] in order to find statistically significant slices among a stream of slices. Lastly, even a handful of problematic slices can be overwhelming to the user, since she may need to take action (e.g., deeper analyses or model debugging) on each slice. Hence, it is important to enable the user to quickly browse through the slices by slice size and effect size. To this end, SliceFinder provides interactive visualization tools for the user to explore the recommended slices.

The following subsections describe the SliceFinder components in detail. Section 3.1 introduces the automated data slicing approaches without false discovery control, Section 3.2 discusses the false discovery control, and Section 3.3 describes the interactive visualization.

3.1 Automated Data Slicing

As mentioned earlier, the goal of this component is to automatically identify problematic slices for model validation. To motivate the development of the two techniques that we mentioned (decision tree and lattice searching), let us first consider a simple baseline approach that identifies the problematic slices through clustering. And then, we discuss two automated data slicing approaches used in SliceFinder that improve on the clustering approach. While the decision tree technique finds a subset of problematic slices that satisfy Definition 1, the lattice search technique finds all of them.

3.1.1 Clustering

The idea is to cluster similar examples together and take each cluster as an arbitrary data slice. If a test model fails on any of the slices, then the user can examine the data examples within or run a more complex analysis to fix the problem. This is an intuitive way to understand the model and its behavior (e.g., predictions) [7], [8], [9]; we can take a similar approach to the automated data slicing problem. The hope is that similar examples would behave similarly even in terms of data or model issues.

Clustering is a reasonable baseline due to its ease of use, but it has major drawbacks: first, it is hard to cluster and explain high dimensional data. We can reduce the dimensionality using principal component analysis (PCA) before clustering, but many features of clustered examples (in its original feature vector) still have high variance or high cardinality of values. Unlike an actual data slice filtered by certain features, this is hard to interpret unless the user can manually go through the examples and summarize the data in a meaningful way. Second, the user has to specify the number of

clusters, which affects crucially the quality of clusters in both metrics and size. As we want slices that are problematic and large (more impact for model quality), this is a key parameter, which is hard to tune. The two techniques that we present next overcome these deficiencies.

3.1.2 Decision Tree Training

To identify more interpretable problematic slices, we train a decision tree that can classify which slices are problematic. The output is a partitioning of the examples into the slices defined by the tree. For example, a decision tree could produce the slices $\{A > v, A \leq v \wedge B > w, A \leq v \wedge B \leq w\}$. For numeric features, this kind of partitioning is natural. For categorical features, a common approach is to use one-hot encoding where all possible values are mapped to columns, and the selected value results in the corresponding column to have a value 1. We can also directly handle categorical features by splitting a node using tests of the form $A = v$ and $A \neq v$. In Section 5.6, we illustrate problematic slices that can be generated from decision tree training.

To use a decision tree, we start from the root slice (i.e., the entire dataset) and go down the decision tree to find the top- k problematic slices in a breadth-first traversal. The decision tree can be expanded one level at a time where each leaf node is split into two children that minimize impurity. The slices of each level are sorted by the \prec ordering and then filtered based on whether they have large-enough effect sizes and are statistically significant. The details of the filtering are similar to lattice searching, which we describe in Section 3.1.3. The searching terminates when either k slices are found or there are no more slices to explore.

The decision tree approach has the advantage that it has a natural interpretation, since the leaves directly correspond to slices. In addition, if the decision tree only needs to be expanded a few levels to find the top- k problematic slices, then the slice searching can be efficient. On the other hand, the decision tree approach optimizes on the classification results and may not find all problematic slices according to Definition 1. For example, if some feature is split on the root node, then it will be difficult to find single-feature slices for other features. In addition, a decision tree always partitions the data, so even if there are two problematic slices that overlap, at most one of them will be found. Another downside is that, if a decision tree gets too deep with many levels, then it starts to become uninterpretable as well [21].

3.1.3 Lattice Searching

The lattice searching approach considers a larger search space where the slices form a lattice, and problematic slices can overlap with one another. We assume that slices only have equality literals, i.e., $\bigwedge_i F_i = v_i$. In contrast to the decision tree training approach, lattice searching can be more expensive because it searches overlapping slices.

Fig. 2 illustrates how slices can be organized as a lattice. Lattice searching performs a breadth-first search and efficiently identifies problematic slices as shown in Algorithm 1. As a pre-processing step, *SliceFinder* takes the training data and discretizes numeric features. For categorical features that contain too many values (e.g., IDs are unique for each example), *SliceFinder* uses a heuristic where it considers up to the M most frequent values and places the rest into an

“other values” bucket. The possible slices of these features form a lattice where a slice S is a parent of every S with one more literal.

Algorithm 1. Lattice Searching Algorithm

Input: Lattice root R , max. number of slices to return k , effect size threshold T , significance level α
Output: Problematic slices S

```

1  $S = []$ 
2  $C = \text{PriorityQueue}()$  /* candidates for significance
   testing sorted by  $\prec$  */
3  $N = []$  /* non-problematic slices */
4  $L = 1$  /* number of literals */
5  $E = \text{EXPANDSLICES}(\{R\}, L)$  /* expand root slice */
6  $W = \alpha$  /* initialize  $\alpha$  wealth */
7 While  $\text{True}$  do
8   for  $\text{slice} \in E$  do
9     if  $\text{EFFECTSIZE}(\text{slice}) \geq T$  then
10        $C.\text{push}(\text{slice})$ 
11     else
12        $N.\text{append}(\text{slice})$ 
13   While  $C$  not empty do
14      $\text{slice} = C.\text{pop}()$ 
15     if  $\text{ISIGNIFICANT}(\text{slice}, W)$  then
16        $S.\text{append}(\text{slice})$ 
17       if  $|S| = k$  then
18         return  $S$ 
19        $W = \text{UPDATEWEALTH}(W, 1)$ 
20     else
21        $N.\text{append}(\text{slice})$ 
22        $W = \text{UPDATEWEALTH}(W, 0)$ 
23    $L += 1$ 
24    $E = \text{EXPANDSLICES}(N, L)$ 
25   if  $E$  is empty then
26     break
27 return  $S$ 
```

SliceFinder finds the top- k interpretable and large problematic slices sorted by the \prec order by traversing the slice lattice in a breadth-first manner, one level at a time. Initially *SliceFinder* considers the slices that are defined with one literal. For each slice, *SliceFinder* checks if it has an effect size at least T (using the *EFFECTSIZE* function) and adds it to the priority queue C , which contains candidate slices that are sorted by the \prec order. Next, *SliceFinder* pops slices from C and tests for statistical significance using the *ISIGNIFICANT* function. The testing can be done using α -investing, which we discuss in Section 3.2. Sorting the slices in the middle of the process using C is important for the α -investing policy used by *SliceFinder* as we explain later.

Each slice that has both a large enough effect size and is statistically significant is added to N and later expanded using the *EXPANDSLICES* function where we generate each new slice by adding a literal, only if the resulting slice is not subsumed by a previously-identified problematic slice. The intuition is that any subsumed (expanded) slice contains a subset of the examples of its parent and is smaller with more filter predicates (less interpretable); thus, we do not expand larger and already problematic slices. By starting from the slices whose predicates are single literals and expanding only non-problematic slices with one additional literal at a time (i.e.,

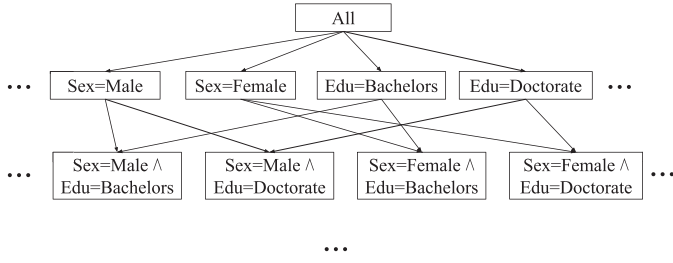


Fig. 2. A lattice hierarchy of slices. In contrast with a decision tree, the search is more exhaustive and covers all possible feature combinations.

top-down search from lower order slices to higher order slices), we can generate a superset of all candidate slices. Depending on whether each slice satisfies the two conditions, *SliceFinder* updates the α -wealth accordingly using the *UPDATEWEALTH* function (details on the updating strategy are discussed in Section 3.2).

Example 2. Suppose there are three features A , B , and C with the possible values $\{a_1\}$, $\{b_1, b_2\}$, and $\{c_1\}$, respectively. Also say $k = 2$, and the effect size threshold is T . Initially, the root slice is expanded to the slices $A = a_1$, $B = b_1$, $B = b_2$, and $C = c_1$, which are inserted into E . Among them, suppose that only $A = a_1$ has an effect size at least T while the others do not. Then $A = a_1$ is added to C for significance testing while the rest are added to N . Next, $A = a_1$ is popped from C and is tested for statistical significance. Suppose the slice is significant and is thus added to S . Since C is now empty, the slices in N are expanded to $B = b_1 \wedge C = c_1$ and $B = b_2 \wedge C = c_1$, which are not subsumed by the problematic slice $A = a_1$. If $B = b_1 \wedge C = c_1$ is larger and has both an effect size at least T and is statistically significant, then the final result is $[A = a_1, B = b_1 \wedge C = c_1]$.

3.1.4 Scalability

SliceFinder optimizes its search by expanding the filter predicate by one literal at a time. Unfortunately, this strategy does not solve the scalability issue of the data slicing problem completely, and *SliceFinder* could still search through an exponential number of slices, especially for large high-dimensional data sets. A possible heuristic is to limit the set of features F to the ones that are of interest to the user before running *SliceFinder*. In addition, *SliceFinder* can take the following two approaches for speeding up search.

Parallelization. For lattice searching, evaluating a given model on a large number of slices one-by-one (sequentially) can be very expensive. In particular, computing the effect sizes is the performance bottleneck. So instead, *SliceFinder* can distribute effect size evaluation jobs (lines 8–12 in Algorithm 1) by keeping separate priority queues E_d for the different number of literals d . The idea is that workers take slices from the current E in a round-robin fashion and evaluate them asynchronously; the workers push slices that have high effect sizes to the priority queue C (for hypothesis testing) as they finish evaluating the slices. The significance testing on the slices in C can be done by a single worker because the slices have already been filtered by effect size, and the significance testing can be done efficiently. In addition, the added memory and communication overheads are

negligible compared to the time for computing the effect sizes. If C is empty, but $|S| < k$, *SliceFinder* moves onto the next queue E_{d+1} and continues searching until $|S| = k$.

For DT, our current implementation does not support parallel learning algorithms for constructing trees. However, there exist a number of highly parallelizable learning processes for decision trees [22], which *SliceFinder* could implement to make DT more scalable.

Sampling. *SliceFinder* can also scale by running on a sample of the entire dataset. The runtime of *SliceFinder* is proportional to the sample size, assuming that the runtime for the test model is constant for each example. By taking a sample, however, we also run the risk of false positives (non-problematic slices that appear problematic) and false negatives (problematic slices that appear non-problematic or completely disappear from the sample) due to a decreased number of examples. Since we are interested in large slices that are more impactful to model quality, we can disregard smaller false negatives that may have disappeared from the sample. In Section 5.5, we show that even for small sample sizes, most of the problematic slices can still be found. In Section 3.2, we perform significance testing to filter slices that falsely appear as problematic or non-problematic.

3.2 False Discovery Control

As *SliceFinder* finds more slices for testing, there is also the danger of finding more “false positives” (Type-1 errors), which are slices that are not statistically significant. *SliceFinder* controls false positives in a principled fashion using α -investing [20]. Given an initial α -wealth (overall Type I error rate) α , α -investing spends this over multiple comparisons, while increasing the budget α towards the subsequent tests with each rejected hypothesis. More formally, let $W(k) > 0$ denote the available α -wealth after k tests have been executed; $W(0)$ is an initial value and typically set to 0.01 or 0.05 [17]. At step j , an α -investing rule sets α_j for testing the j th hypothesis based on $W(j-1)$. If $p_j \leq \alpha_j$, the test rejects the hypothesis, and an α -wealth of w (typically set to $W(0)$) is earned. This so called pay-out helps the procedure become less conservative and puts more weight on null hypotheses that are more likely to be faulty. If $p_j > \alpha_j$, the hypothesis is accepted and its available α -wealth decreases by $\alpha_j/(1 - \alpha_j)$:

$$W(t) - W(t-1) = \begin{cases} w & \text{if } p_j \leq \alpha_j, \\ -\frac{\alpha_j}{1-\alpha_j} & \text{if } p_j > \alpha_j. \end{cases}$$

The testing procedure halts when the remaining α -wealth reaches 0. α investing effectively controls the marginal false discovery rate at level α :

$$\frac{\mathbb{E}(V)}{\mathbb{E}(R)} \leq \alpha$$

Here, V is the number of false discoveries and R the number of total discoveries returned by the procedure. *SliceFinder* uses α -investing, mainly because it allows more interactive multiple hypothesis error control with an unspecified number of tests in any order. On the contrary, more restricted multiple hypothesis error control techniques, such as Bonferroni correction and Benjamini-Hochberg procedure [10] fall

short as they require the total number of tests m in advance or become too conservative as m grows large.

While there are different α -investing policies [17] for testing a sequence of hypotheses, we use a policy called *Best-foot-forward*. Recall our exploration strategy orders slices by decreasing slice size and effect size. As a result, the initial slices also tend to be statistically significant as well. The Best-foot-forward policy also assumes that many of the rejected hypotheses are found early on and aggressively invests α -wealth on each hypothesis. If the most recently rejected hypothesis is the k^* th hypothesis, the Best-foot-forward policy invests heavily in the $(k^* + 1)$ th hypothesis testing as:

$$\alpha_j = \frac{W(j-1)}{1+j-k^*}$$

That is, the policy invests half of the current α -wealth for next $(j = k^* + 1)$ hypothesis testing. If the initial hypotheses are likely to be rejected, then the total α -wealth will increase, enabling more rejections in subsequent testing with high α values. By using α -investing with the Best-foot-forward policy, *SliceFinder* becomes interactive where it can find statistically significant slices from a stream of slices.

3.3 Interactive Visualization Tool

Users can interact with *SliceFinder* through the GUI shown in Fig. 3. The scatter plot on the left supports quick browsing while the table on the right shows details of selected slices. On the bottom are configurable sliders for adjusting k and T . *SliceFinder* materializes all the problematic slices ($\phi \geq T$) as well as the non-problematic slices ($\phi < T$) searched already. If T decreases, we just need to reiterate the slices explored until now to find the top- k slices. If T increases, then the current slices may not be sufficient, depending on k , so we continue searching the slice tree or lattice. This interaction is possible because *SliceFinder* looks for the top- k slices in a top-down manner.

4 USING SliceFinder FOR MODEL FAIRNESS

In this section, we look at model fairness [23] as a potential use case of *SliceFinder* where identifying problematic slices can be a preprocessing step before more sophisticated analyses on fairness on the slices. As machine learning models are increasingly used in sensitive applications, such as predicting whether individuals will default on loans [24], commit a crime [25], or survive intensive hospital care [26], it is essential to make sure the model performs equally well for all demographics to avoid discrimination. However, models may fail this property for various reasons: bias in data collection, insufficient data for certain slices, limitations in the model training, to name a few cases.

Model fairness has various definitions depending on the application and is thus non-trivial to formalize [27]. While many metrics have been proposed [23], [24], [28], [29], [30], [31], [32], there is no widely-accepted standard, and some definitions are even at odds. In this paper, we focus on one of the common definitions called disparate mistreatment [31], which directly fits into the *SliceFinder* framework.

Disparate mistreatment requires a predictor \hat{y} (e.g., a classification model h in our case) to have the same

misclassification rates for different groups of people having different values of the protected or sensitive feature $A \in \{0, 1\}$. Different misclassification measures including true positive rates (*tpr*) or false negative rates (*fmr*) are possible, but the most commonly-used metric is the overall misclassification error (*omr*). In the case of binary classification ($y \in \{0, 1\}$), disparate mistreatment becomes:

$$Pr\{\hat{y} \neq y | A = 0\} = Pr\{\hat{y} \neq y | A = 1\}$$

The problematic slices with $\phi \geq T$ suffer from higher loss (lower model accuracy in case of log loss) compared to the counterparts, which implies disparate mistreatment. A model with such problematic slices is considered biased.

SliceFinder can be extended to other model fairness definitions including the widely-used disparate impact [28]. A model does not have disparate impact if the probability that the model assigns to the favorable outcome, $\hat{y} = 1$, is similar for different groups. A common criteria to determine disparate impact is the 80 percent rule:

$$\min\left(\frac{Pr\{\hat{y} = 1 | A = 0\}}{Pr\{\hat{y} = 1 | A = 1\}}, \frac{Pr\{\hat{y} = 1 | A = 1\}}{Pr\{\hat{y} = 1 | A = 0\}}\right) \geq 0.8$$

We can extend *SliceFinder* to search for slices that introduce disparate impact by violating the 80 percent rule in a straightforward fashion.

5 EXPERIMENTS

In this section, we compare the two *SliceFinder* approaches (decision tree and lattice search) with the baseline (clustering). For the clustering approach, we use the k -means algorithm. We address the following key questions:

- How accurate and efficient is *SliceFinder*?
- What are the trade-offs between the slicing techniques?
- What is the impact of adjusting the effect size threshold T ?
- Are the identified slices interpretable enough to understand the model's performance?
- How effective is false discovery control using α -investing?

5.1 Experimental Setup

We used the following two problems with different datasets and models to compare how the three different slicing techniques – lattice search (LS), decision tree (DT), and clustering (CL) – perform in terms of recommended slice quality as well as their interpretability.

- *Census Income Classification*: We trained a random forest classifier (Example 1) to predict whether the income exceeds \$50K/yr based on the UCI census data [33]. There are 15 features and 30K examples. The features (including the discretized ones) contain 2–118 categories.
- *Credit Card Fraud Detection*: We trained a random forest classifier to predict fraudulent transactions among credit card transactions [34]. This dataset contains transactions that occurred over two days,

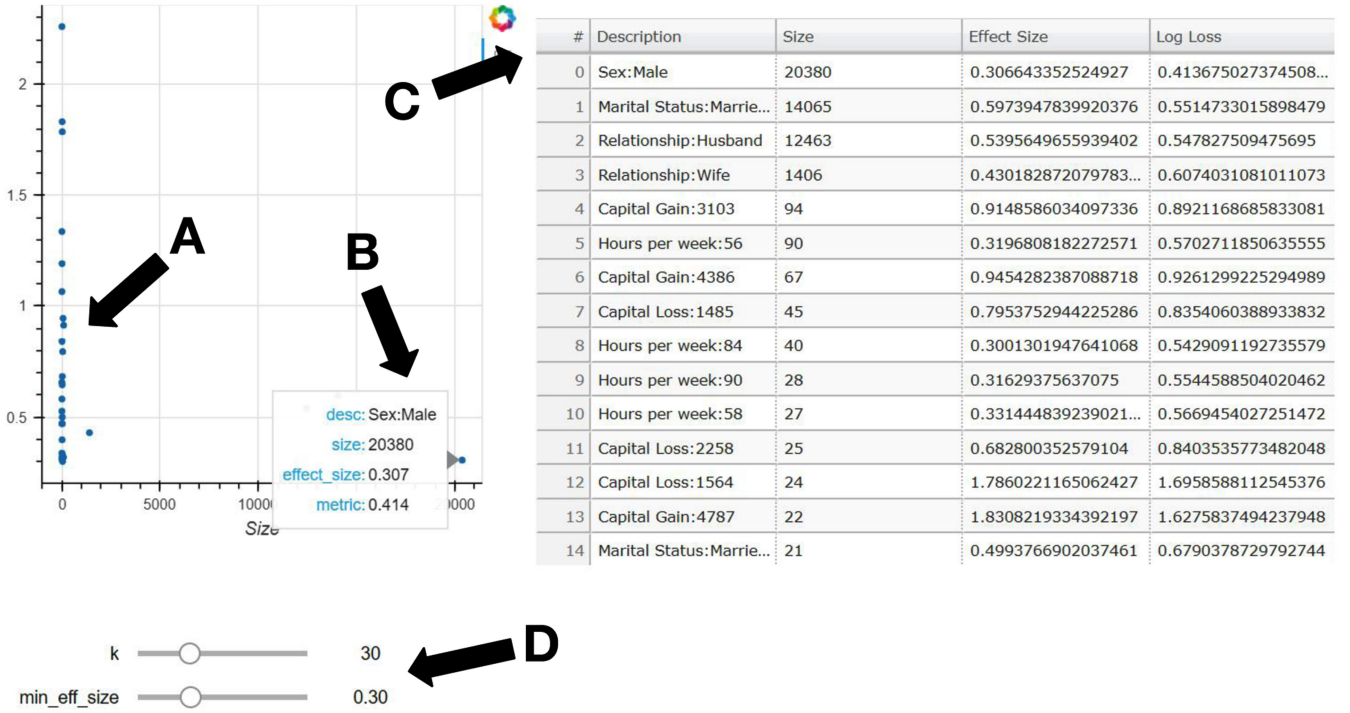


Fig. 3. The SliceFinder GUI helps users quickly browse through problematic slices by effect size and slice size on a scatter plot (A) and see a slice summary by hovering over any point (B); the user can sort slices by any metric and select on the scatter plot or table view. The selections are highlighted on the linked views (C). The user can also explore the top- k large problematic slices by varying the effect size threshold using the slider (min_eff_size) on the bottom left corner (D).

where we have 492 frauds out of 284k transactions (examples), each with 29 numeric features. Because the data set is heavily imbalanced, we first under-sample non-fraudulent transactions to balance the data. This leaves a total of 984 transactions in the balanced dataset. For the LS experiments, the values of each feature are discretized into 10 buckets.

As we shall see, the two datasets – Census Income and Credit Card Fraud – have different characteristics and are thus useful for comparing the behaviors of the decision tree and lattice search algorithms. In addition, we also use a synthetic dataset when necessary. The main advantage of using synthetic data is that it gives us more insights into the operations of SliceFinder. In Sections 5.2, 5.3, 5.4, 5.5, 5.6, we assume that all slices are statistically significant for simplicity and separately evaluate statistical significance in Section 5.7.

Accuracy Measure. Since problematic slices may overlap, we define *precision* to be the fraction of examples in the union of the slices identified by the algorithm being evaluated that also appear in actual problematic slices. Similarly, *recall* is defined as the fraction of the examples in the union of actual problematic slices that are also in the identified slices. Finally, *accuracy* is the harmonic mean of precision and recall.

5.2 Problematic Slice Identification

An important question to answer is whether SliceFinder can indeed find the most problematic slices, in the user's point of view. Unfortunately for the real datasets, we do not know what are the true problematic slices, which makes our evaluation challenging. Instead, we *add new problematic slices* by randomly perturbing labels and focus on finding those slices. While SliceFinder may find both new and existing

problematic slices, our evaluation will only be whether SliceFinder finds the new problematic slices.

We first experiment on a synthetic dataset and compare the performances of LS, DT, and CL. We then experiment on the real datasets and show similar results.

5.2.1 Synthetic Data

We generate a simple synthetic dataset where the generated examples have two discretized features F_1 and F_2 and can be classified into two classes – 0 and 1 – perfectly. We make the model use this decision boundary and do not change it further. Then we add problematic slices by choosing random possibly-overlapping slices of the form $F_1 = A$, $F_2 = B$, or $F_1 = A \wedge F_2 = B$. For each slice, we flip the labels of the examples with 50 percent probability. Note that this perturbation results in the worst model accuracy possible.

Fig. 4a shows the accuracy comparison of LS, DT, and CL on synthetic data. As the number of recommendations increases, LS consistently has a higher accuracy than DT because LS is able to better pinpoint the problematic slices including overlapping ones while DT is limited in the sense that it only searches non-overlapping slices. For CL, we only evaluated the clusters with effect sizes at least T . Even so, the accuracy is much lower than those of LS and DT.

5.2.2 Real Data

We also perform a similar experiment using the Census Income dataset where we generate new problematic slices on top of the existing data by randomly choosing slices and flipping labels with 50 percent probability. Compared to the synthetic data, the existing data may also have problematic slices, which we do not evaluate because we do not know

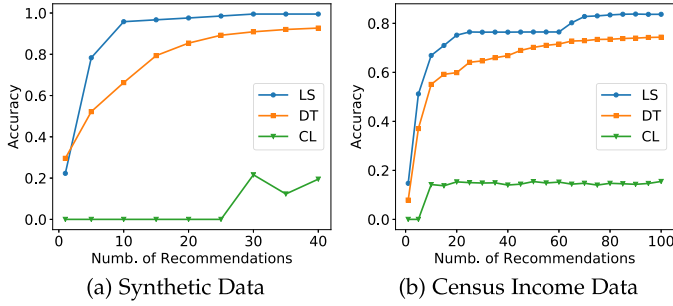


Fig. 4. Accuracy comparison of finding problematic slices using (a) synthetic data and (b) real data.

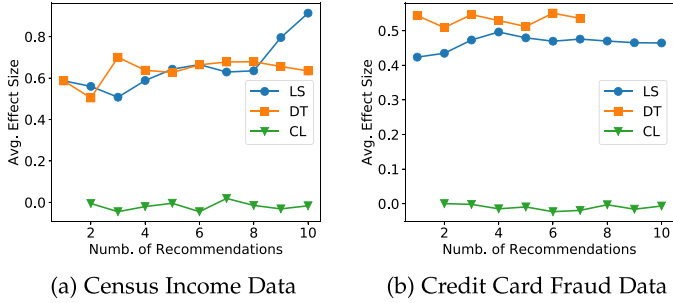


Fig. 5. Effect size comparisons between different data slicing approaches ($T = 0.4$).

what they are. Fig. 4b shows similar comparison results between LS, DT, and CL. The accuracies of LS and DT are lower than those in the synthetic data experiments because some of the identified slices may be problematic slices in the existing data, but are considered incorrect when evaluated.

5.3 Large Problematic Slices

Figs. 5 and 6 show how LS and DT outperform CL in terms of average slice size and average effect size on the real datasets. CL starts with the entire dataset where the number of clusters (i.e., recommendations) is 1. CL produces large clusters that have very low effect sizes where the average is around 0.0 and sometimes even negative, which means some slices are not problematic. The CL results show that grouping similar examples does not necessarily guide users to problematic slices. In comparison, LS and DT find smaller slices with effect sizes above the threshold $T = 0.4$. In subsequent experiments, we do not make comparisons with CL because of its poor results in finding problematic slices.

LS and DT show different behaviors depending on the given dataset. When running on the Census Income data, both LS and DT are able to easily find up to $k = 10$ problematic slices with similar effect sizes. Since LS generally has a larger search space than DT where it also considers overlapping slices, it is able to find larger slices as a result. When running on the Credit Card Fraud data, DT has a harder time finding enough problematic slices. The reason is that DT initially finds a large problematic slice, but then needs to generate many levels of the decision tree to find additional problematic slices because it only considers non-overlapping slices. Since a decision tree is designed to partition data to minimize impurity, the slices found deeper down the tree tend to be smaller and “purer,” which means the problematic ones have higher effect sizes. Lastly, DT could not find more than 7 problematic slices because the leaf nodes were too

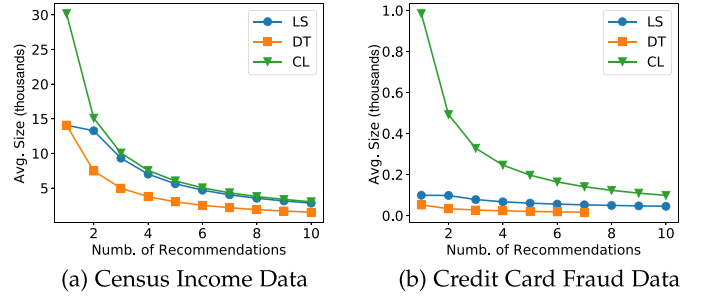


Fig. 6. Average slice size (unit is 1000) comparisons between different data slicing approaches ($T = 0.4$).

small to split further. These results show that, while DT may search a level of a decision tree faster than LS searching a level of a lattice, it may have to search more levels of the tree to make the same number of recommendations.

5.4 Adjusting Effect Size Threshold T

Fig. 7 shows the impact of adjusting the effect size threshold T on LS and DT. For a low T value, there are more slices that can be problematic. Looking at the Census Income data, LS indeed finds larger slices than those found by DT, although they have relatively smaller effect sizes as a result. As T increases, LS is forced to search smaller slices that have high-enough effect sizes. Since LS still has a higher search space than DT, it does find slices with higher effect sizes when T is at least 0.4. The Credit Card Fraud data shows a rather different comparison. For small T values, recall that DT initially finds a large problematic slice, which means the average size is high, and the effect size small. As T increases, DT has to search many levels of the decision tree to find additional problematic slices. These additional slices are much smaller, which is why there is an abrupt drop in average slice size. However, the slices have higher effect sizes, which is why there is also a corresponding jump in the average effect size.

5.5 Scalability

We evaluate the scalabilities of LS and DT against different sample fractions, degree of parallelization, and the number of top- k slices to recommend. All experiments were performed on the Census Income dataset.

Fig. 8 shows how the runtimes of LS and DT change versus the sampling fraction. For both algorithms, the runtime increases almost linearly with the sample size. We also measure the relative accuracy of the two algorithms where we compare the slices found in a sample with the slices found in the full dataset. For a sample fraction of $1/128$, both LS and DT maintain a high relative accuracy of 0.88. These results show that it is possible to find most of the problematic slices using a fraction of the data, about two orders of magnitude faster.

Fig. 9a illustrates how SliceFinder can scale with parallelization. LS can distribute the evaluation (e.g., effect size computation) of the slices with the same number of filter predicates to multiple workers. As a result, for the full Census Income data, increasing the number of workers results in better runtime. As we mentioned in 3.1.4, SliceFinder only supports parallel computing for the effect size evaluation jobs, which is why Fig. 9a does not show linear scaling. Notice that the marginal runtime improvement decreases as we add more workers. The results for DT are not shown here

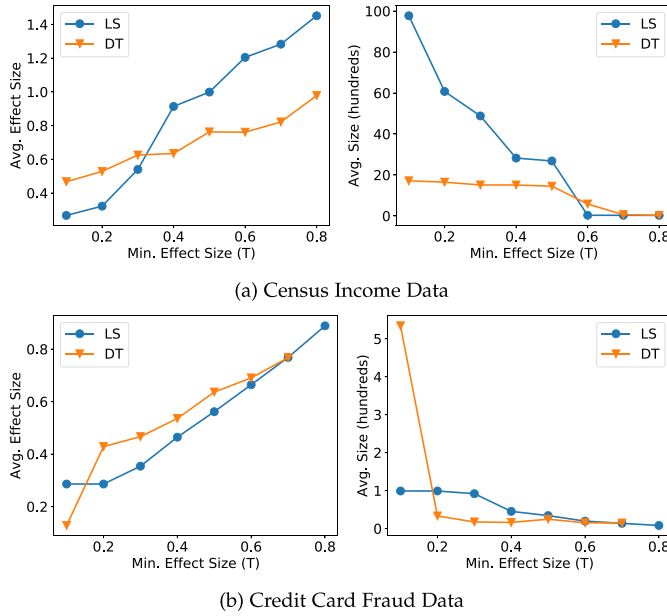


Fig. 7. The impact of adjusting the effect size threshold T on average slice size and average effect size.

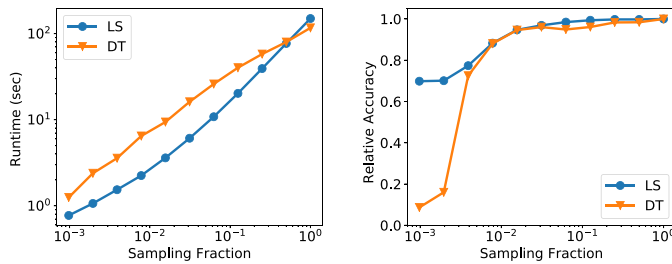


Fig. 8. SliceFinder (LS, DT) runtime (on a single node) and accuracy results using different sample sizes (Census Income data).

because the current implementation does not support parallel DT model training.

Fig. 9b compares the runtimes of LS and DT when the number of top- k recommendations increases. For small k values less than 5, DT is faster because it searches fewer slices to find k problematic ones. However, as k increases, DT needs to search through many levels of a decision tree and starts to run relatively slower than LS. Meanwhile, LS only searches the next level of the lattice if k is at least 70 at which point DT is again faster. Thus, whether LS or DT is faster depends on k and how frequently the problematic slices occur.

5.6 Interpretability

An important feature of SliceFinder is that it can find interpretable slices that can help a user understand and describe the model's behavior using a few common features. A user without SliceFinder may have to go through all the misclassified examples (or clusters of them) manually to see if the model is biased or failing.

Table 2 shows top-5 problematic slices from the two datasets using LS and DT. Looking at the top-5 slices found by LS from the Census Income data, the slices are easy to interpret with a few number of common features. We see that the `MaritalStatus = Married-civ-spouse` slice has the largest size as well as a large effect size, which indicates that the model

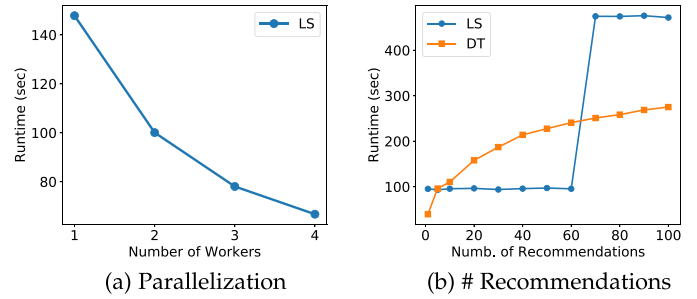


Fig. 9. (a) SliceFinder runtime results with increasing number of (a) parallel workers and (b) recommendations (Census Income data).

can be improved for this slice. It is also interesting to see that the model fails for the people who are husbands or wives, but not for other relationships: own-child, not-in-family, other-relative, and unmarried. We also see slices with high capital gains tend to be problematic in comparison to the common case where the value is 0. In addition, the top-5 slices found by DT from the Census Income data can also be interpreted in a straightforward way, although having more literals makes the interpretation more tedious. Finally, the top-5 slices from the Credit Card Fraud data are harder (but still reasonable) to interpret because many feature names are anonymized (e.g., V14).

In general, we cannot always assume that features are easily interpretable to humans. For example, one may use numerous n -gram or skip-gram features when classifying large text documents. In the extreme case, a feature may be intentionally misleading to avoid interpretability. Extending SliceFinder to uninterpretable features is thus an interesting future work.

5.7 False Discovery Control

Even for a small data set (or sample), there can be an overwhelming number of problematic slices. The goal of Slice Finder is to bring the user's attention to a handful of large problematic slices; however, if the sample size is small, most slices would contain fewer examples, and thus, it is likely that many slices and their effect size measures are seen by chance. In such a case, it is important to prevent false discoveries (e.g., non-problematic slices appear as problematic where $\phi \geq T$ due to sampling bias).

For evaluation, we use the Census Income data and compare the results of Bonferroni correction (BF), the Benjamini-Hochberg procedure (BH), and α -investing (AI) using two standard measures: *false discovery rate*, which was described in Section 3.2, and *power* [17], which is the probability that the tests correctly reject the null hypothesis. We use the same setting in Section 5.2 for generating problematic slices. We then run Slice Finder and take the top-70 slices for the false discovery control and power evaluation. We used $k = 70$ because it is large enough to observe many false discoveries. The smaller the k value is, the fewer the false discoveries.

The results in Fig. 10 show that, as the α -value (or wealth when using AI) increases up to 0.01, AI and BH have higher FDR results than BF, but higher power results as well. When measuring the accuracy of slices, AI slightly outperforms both BH and BF because it invests its α more effectively using the Best-foot-forward policy. In comparison, BF is conservative and has a high false-discovery rate (which results in

TABLE 2
Top-5 Slices Found by LS and DT from the Census Income and Credit Card Fraud Datasets

Slice	# Literals	Size	Effect Size
LS slices from Census Income data			
MaritalStatus = Married-civ-spouse	1	14065	0.58
Relationship = Husband	1	12463	0.52
Relationship = Wife	1	1406	0.46
CapitalGain = 3103	1	94	0.87
CapitalGain = 4386	1	67	0.94
DT slices from Census Income data			
MaritalStatus = Married-civ-spouse	1	14065	0.58
MaritalStatus \neq Married-civ-spouse \rightarrow CapitalGain \geq 7298 \rightarrow CapitalGain $<$ 8614 \rightarrow Education-Num $<$ 13	4	7	0.58
MaritalStatus \neq Married-civ-spouse \rightarrow CapitalGain $<$ 7298 \rightarrow Education-Num \geq 13 \rightarrow Age \geq 28 \dots \rightarrow Hoursperweek \geq 44	5	855	0.43
MaritalStatus \neq Married-civ-spouse \rightarrow CapitalGain $<$ 7298 \rightarrow Education-Num \geq 13 \rightarrow Age $<$ 28 \dots \rightarrow CapitalLoss \geq 2231	5	5	1.07
MaritalStatus \neq Married-civ-spouse \rightarrow CapitalGain $<$ 7298 \rightarrow Education-Num \geq 13 \rightarrow Age \geq 28 \dots \rightarrow Hoursperweek $<$ 44 \rightarrow Education-Num \geq 15	6	101	0.47
LS slices from Credit Card Fraud data			
V14 = -3.69 - -1.00	2	98	0.45
V7 = 0.94 - 23.48 \rightarrow V10 = -2.16 - -0.87	3	29	0.41
V1 = 1.13 - 1.74 \rightarrow V25 = 0.48 - 0.71	4	28	0.54
V7 = 0.94 - 23.48 \rightarrow Amount = 270.54 - 4248.34	4	28	0.53
V10 = -2.16 - -0.87 \rightarrow V17 = 0.92 - 6.74	5	27	0.44
DT slices from Credit Card Fraud data			
V14 $<$ -2.17 \rightarrow V10 \geq -1.52	2	31	0.60
V14 \geq -2.17 \rightarrow V4 \geq 0.76 \rightarrow V12 $<$ -0.42	3	59	0.48
V14 \geq -2.17 \rightarrow V4 $<$ 0.76 \rightarrow V14 $<$ -0.93 \rightarrow V2 $<$ 1.04	4	23	0.42
V14 \geq -2.17 \rightarrow V4 $<$ 0.76 \rightarrow V14 \geq -0.93 \rightarrow Amount \geq 320	4	18	0.52
V14 \geq -2.17 \rightarrow V4 \geq 0.76 \rightarrow V12 \geq -0.42 \rightarrow Amount \geq 1 \rightarrow V17 \geq 1.68	5	6	0.63

When denoting a slice from a decision tree, we use the \rightarrow notation to order the literals by level.

lower accuracy), and BH does not exploit the fact that the earlier slices are more likely to be problematic as AI does. The more important advantage of AI is that it is the only technique that works in an interactive setting.

6 RELATED WORK

In practice, the overall performance metrics can mask the issues on a more granular-level, and it is important to validate the model accordingly on smaller subsets/sub-populations of data (slices). While a well-known problem, the existing tools are still primitive in that they rely on domain experts to pre-define important slices. State-of-art tools for machine learning model validation include Facets [35], which can be used to discover bias in the data, TensorFlow Model Analysis (TFMA), which slices data by an input feature dimension for a more granular performance analysis [6], and MLCube [5], which provides manual exploration of slices and can both evaluate a single model or compare two models. While the above tools are manual, SliceFinder complements them by automatically finding slices useful for model validation.

There are several other lines of work related to this problem, and we list the most relevant work to SliceFinder.

Data Exploration. Online Analytical Processing (OLAP) has been tackling the problem of slicing data for analysis, and the techniques deal with the problem of large search space (i.e., how to efficiently identify data slices with certain properties). For example, Smart Drilldown [36] proposes an OLAP drill down process that returns the top- k most “interesting” rules such that the rules cover as many records as possible while

being as specific as possible. Intelligent rollups [37] goes the other direction where the goal is to find the broadest cube that share the same characteristics of a problematic record. A related technique to OLAP is explanation tables [38] where the goal is to summarize a binary attribute (e.g., whether someone has a high salary) in a table by aggregating other dimension attributes. In comparison, SliceFinder finds subsets of the entire data, on which the model underperforms, without having to evaluate the model on all the possible subsets. This is different from general OLAP operations based on cubes with pre-summarized aggregates, and the OLAP algorithms cannot be directly used.

Model Understanding. Understanding a model and its behavior is a broad topic that is being studied extensively [8], [9], [21], [39], [40], [41]. For example, LIME [8] trains interpretable linear models on local data and random noise to see which features are prominent. Anchors [9] are high-precision

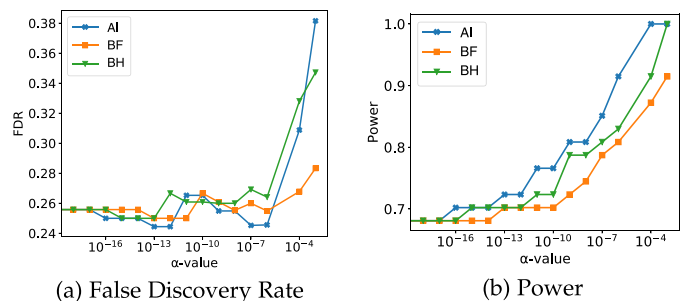


Fig. 10. (a) False discovery rate and (b) power comparison of the Bonferroni, Benjamini Hochberg, and α -investing techniques (Census Income data). The y-axes of (a) and (b) start from 0.24 and 0.65, respectively.

rules that provide local and sufficient conditions for a black-box model to make predictions. In comparison, SliceFinder is a complementary tool to identify subsets of the data where the model is performing relatively worse than other parts. As a result, there are certain applications (e.g., model fairness) that benefit more from slices. PALM [7] isolates a small set of training examples that have the greatest influence on the prediction by approximating a complex model into an interpretable meta-model that partitions the training data and a set of sub-models that approximate the patterns within each pattern. PALM expects as input the problematic example and a set of features that are explainable to the user. In comparison, SliceFinder finds large, significant, and interpretable slices without requiring user input. Influence functions [42] have been used to compute how each example affects model behavior. In comparison, SliceFinder identifies interpretable slices instead of individual examples. An interesting research direction is to extend influence functions to slices and quantify the impact of slices on the overall model quality.

Feature Selection. SliceFinder is a model validation tool, which comes after model training. It is important to note that this is different from feature selection [43], [44] in model training, where the goal is often to identify and (re-)train on the most correlated features (dimensions) to the target label (i.e., finding representative features that best explain model predictions). Instead, SliceFinder identifies a few common feature values that describe subsets of data with significantly high error concentration for a given model; this, in turn, could help the user to interpret hidden model performance issues that are masked by good overall model performance metrics.

7 CONCLUSION

We have proposed SliceFinder as a tool for efficiently and accurately finding large, significant, and interpretable slices. The techniques are relevant to model validation in general, but also to model fairness and fraud detection where human interpretability is critical to understand model behavior. We have proposed two complementing approaches for slice finding: decision tree training, which finds non-overlapping slices, and lattice searching, which finds possibly-overlapping slices. We also provide an interactive visualization front-end to help users quickly browse through a handful of problematic slices.

In the future, we would like to improve SliceFinder to better discretize numeric features and support the merging and summarization of slices. We would also like to “repair” a model if there are problematic slices by selectively collecting more data for those slices using weak supervision and then retraining the model. We would also like to deploy Slice Finder to production machine learning platforms and conduct a user study on how helpful the slices are for explaining and debugging models.

ACKNOWLEDGMENTS

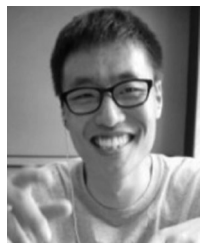
Steven Euijong Whang and Ki Hyun Tae were supported by a Google AI Focused Research Award and by the Engineering Research Center Program through the National Research

Foundation of Korea (NRF) funded by the Korean Government MSIT (NRF-2018R1A5A1059921).

REFERENCES

- [1] D. Baylor, E. Breck, H.-T. Cheng, N. Fiedel, C. Y. Foo, Z. Haque, S. Haykal, M. Ispir, V. Jain, L. Koc, et al., “TFX: A tensorflow-based production-scale machine learning platform,” in *Proc. 23rd ACM SIGKDD Int. Conf.*, 2017, pp. 1387–1395.
- [2] F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” *arXiv preprint arXiv:1702.08608*, 2017.
- [3] M. Lichman, “UCI machine learning repository,” Irvine, CA: University of California, School of Information and Computer Science, 2013, <http://archive.ics.uci.edu/ml/>
- [4] H. B. McMahan, G. Holt, D. Sculley, M. Young, D. Ebner, J. Grady, L. Nie, T. Phillips, E. Davydov, D. Golovin, et al., “Ad click prediction: A view from the trenches,” in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2013, pp. 1222–1230.
- [5] M. Kahng, D. Fang, and D. H. P. Chau, “Visual exploration of machine learning results using data cube analysis,” in *Proc. Workshop Human-In-the-Loop Data Anal.*, 2016, Art. no. 1.
- [6] “Introducing tensorflow model analysis,” 2018. [Online]. Available: <https://medium.com/tensorflow/introducing-tensorflow-model-analysis-scalable-sliced-and-full-pass-metrics-5cde7baf0b7b>
- [7] S. Krishnan and E. Wu, “Palm: Machine learning explanations for iterative debugging,” in *Proc. 2nd Workshop Human-In-the-Loop Data Anal.*, 2017, pp. 4:1–4:6.
- [8] M. T. Ribeiro, S. Singh, and C. Guestrin, “‘Why should I trust you?’: Explaining the predictions of any classifier,” in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2016, pp. 1135–1144.
- [9] M. T. Ribeiro, S. Singh, and C. Guestrin, “Anchors: High-precision model-agnostic explanations,” in *Proc. 32nd AAAI Conf. Artif. Intell.*, 2018, pp. 1527–1535.
- [10] Y. Benjamini and Y. Hochberg, “Controlling the false discovery rate: A practical and powerful approach to multiple testing,” *J. Roy. Statistical Soc. Series B (Methodological)*, vol. 57, no. 1, pp. 289–300, 1995.
- [11] N. Polyzotis, S. Roy, S. E. Whang, and M. Zinkevich, “Data lifecycle challenges in production machine learning: A survey,” *SIGMOD Rec.*, vol. 47, no. 2, pp. 17–28, Jun. 2018.
- [12] N. Polyzotis, S. Roy, S. E. Whang, and M. Zinkevich, “Data management challenges in production machine learning,” in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 1723–1726.
- [13] Y. Chung, T. Kraska, N. Polyzotis, K. H. Tae, and S. E. Whang, “Slice finder: Automated data slicing for model validation,” *Proc. 35th IEEE Int. Conf. Data Eng.*, 2019.
- [14] Y. Chung, T. Kraska, N. Polyzotis, and S. E. Whang, “Slice finder: Automated data slicing for model interpretability,” *Proc. SysML Conf.*, 2018, available on: <http://www.sysml.cc/2018/>
- [15] G. M. Sullivan and R. Feinn, “Using effect size or why the p value is not enough,” *J. Graduate Med. Edu.*, vol. 4, no. 3, pp. 279–282, 2012.
- [16] B. L. Welch, “The generalization of ‘student’s’ problem when several different population variances are involved,” *Biometrika*, vol. 34, pp. 28–35, 1947.
- [17] Z. Zhao, L. D. Stefani, E. Zraggen, C. Binnig, E. Upfal, and T. Kraska, “Controlling false discoveries during interactive data exploration,” in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 527–540.
- [18] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. New York, NY, USA: Academic, 1988.
- [19] W. McKinney, “pandas: A foundational python library for data analysis and statistics,” *Python High Perform. Sci. Comput.*, 2011.
- [20] D. Foster and B. Stine, “Alpha-investing: A procedure for sequential control of expected false discoveries,” *J. Roy. Statistical Soc. Series B (Methodological)*, vol. 70, no. 2, pp. 429–444, 2008.
- [21] A. A. Freitas, “Comprehensible classification models: A position paper,” *SIGKDD Explorations Newslett.*, vol. 15, no. 1, pp. 1–10, Mar. 2014.
- [22] A. Srivastava, E.-H. Han, V. Kumar, and V. Singh, “Parallel formulations of decision-tree classification algorithms,” in *High Performance Data Mining*. New York, NY, USA: Springer, 1999, pp. 237–261.
- [23] R. K. E. Bellamy, K. Dey, and M. Hind, et al., “AI fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias,” *CoRR*, vol. abs/1810.01943, 2018.

- [24] M. Hardt, E. Price, and N. Srebro, "Equality of opportunity in supervised learning," in *Proc. 30th Int. Conf. Neural Inf. Process. Syst.*, 2016, pp. 3315–3323.
- [25] "Machine bias," 2006. [Online]. Available: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [26] M. Ghassemi, T. Naumann, F. Doshi-Velez, N. Brimmer, R. Joshi, A. Rumshisky, and P. Szolovits, "Unfolding physiological state: Mortality modelling in intensive care units," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2014, pp. 75–84.
- [27] S. Barocas and M. Hardt, "Fairness in machine learning," *NIPS Tutorial*, 2017, <http://fairml.how>
- [28] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness through awareness," in *Proc. 3rd Innovations Theoretical Comput. Sci. Conf.*, 2012, pp. 214–226.
- [29] J. M. Kleinberg, S. Mullainathan, and M. Raghavan, "Inherent trade-offs in the fair determination of risk scores," in *Proc. ACM Int. Conf. Meas. Model. Comput. Syst.*, 2017, pp. 43:1–43:23.
- [30] M. Feldman, S. A. Friedler, J. Moeller, C. Scheidegger, and S. Venkatasubramanian, "Certifying and removing disparate impact," in *Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2015, pp. 259–268.
- [31] M. G. Rodriguez, K. P. Gummadi, M. B. Zafar, and I. Valera, "Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment," in *WWW*, 2017.
- [32] M. G. Rodriguez, K. P. Gummadi, M. B. Zafar, and I. Valera, "Fairness constraints: Mechanisms for fair classification," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, 2017, pp. 962–970.
- [33] R. Kohavi, "Scaling up the accuracy of naive-bayes classifiers: A decision-tree hybrid," in *Proc. 2nd Int. Conf. Knowl. Discovery Data Mining*, 1996, vol. 96, pp. 202–207.
- [34] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in *Proc. IEEE Symp. Series Comput. Intell.*, 2015, pp. 159–166.
- [35] "Facets overview," 2017. [Online]. Available: <https://research.googleblog.com/2017/07/facets-open-source-visualization-tool.html>
- [36] M. Joglekar, H. Garcia-Molina, and A. Parameswaran, "Interactive data exploration with smart drill-down," in *Proc. IEEE 32nd Int. Conf. Data Eng.*, 2016, pp. 906–917.
- [37] G. Sathe and S. Sarawagi, "Intelligent rollups in multidimensional olap data," in *Proc. 27th Int. Conf. Very Large Data Bases*, 2001, pp. 531–540.
- [38] K. E. Gebaly, A. Parag, G. Lukasz, K. Flip, and S. Divesh, "Interpretable and informative explanations of outcomes," *Proc. VLDB Endowment*, no. 1, pp. 61–72, 2014.
- [39] P. Tamagnini, J. Krause, A. Dasgupta, and E. Bertini, "Interpreting black-box classifiers using instance-level visual explanations," in *Proc. 2nd Workshop Human-In-the-Loop Data Analytics*, 2017, pp. 6:1–6:6.
- [40] O. Bastani, C. Kim, and H. Bastani, "Interpreting blackbox models via model extraction," *CoRR*, vol. abs/1705.08504, 2017.
- [41] H. Lakkaraju, E. Kamar, R. Caruana, and J. Leskovec, "Interpretable & explorable approximations of black box models," *CoRR*, vol. abs/1707.01154, 2017.
- [42] P. W. Koh and P. Liang, "Understanding black-box predictions via influence functions," in *Proc. 34th Int. Conf. Mach. Learn. - Vol. 70*, 2017, pp. 1885–1894.
- [43] M. Charikar, V. Guruswami, R. Kumar, S. Rajagopalan, and A. Sahai, "Combinatorial feature selection problems," in *Proc. 41st Annu. Symp. Found. Comput. Sci.*, 2000, pp. 631–640.
- [44] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *J. Mach. Learn. Res.*, vol. 3, no. Mar, pp. 1157–1182, 2003.



Yeounoh Chung received the BS degree in electrical and computer engineering and the ME degree in computer science from Cornell University, in 2008 and 2009, respectively, and the PhD degree in computer science from Brown University, in 2018. He is a senior data scientist with Apple Inc. While at Brown, he worked on various data analytics and engineering projects around uncertainty in big data analytics.



Tim Kraska received the PhD degree from ETH Zurich. He is an associate professor of electrical engineering and computer science, MIT's Computer Science and Artificial Intelligence Laboratory. Currently, his research focuses on building systems for machine learning, and using machine learning for systems. Before joining MIT, he was an assistant professor with Brown University, spent time with Google Research, and was a post-doc with the AMPLab, UC Berkeley.



Neoklis Polyzotis received the PhD degree in computer sciences from the University of Wisconsin at Madison and the diploma in engineering from the National Tech. University of Athens, Greece. He is a research scientist with Google Research, where he currently leads the data-management projects in Google's TensorFlow Extended (TFX) platform. His interests include data management for machine learning, enterprise data search, and interactive data exploration. Before joining Google, he was a professor with UC Santa Cruz.



Ki Hyun Tae received the BS degree in electrical engineering from KAIST, in 2018. He is working toward the MS degree in the School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST). His current research interests include big data - AI integration, big data analytics, and AI fairness.



Steven Euijong Whang received the BS degree in computer science from Korea Advanced Institute of Science and Technology (KAIST), in 2003, and the PhD degree in computer science from Stanford University, in 2012. He is an assistant professor with the School of Electrical Engineering, KAIST. His research interests include big data - AI integration, big data analytics, and big data systems. Previously, he was a research scientist with Google Research from December 2012 to January 2018 and co-developed the data infrastructure of the TensorFlow Extended (TFX) machine learning platform. He is a recipient of the Google AI Focused Research Award in 2018, the first in Asia. He is a senior member of the IEEE.

► For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/csdl.