1 Introduction

Model interpretation, or explanation of a machine learning classifier, aims to extract generalizable knowledge from a trained classifier into a human-understandable format, for various purposes such as model assessment, debugging and trust. From a computational viewpoint, it is formulated as approximating the target classifier using a simpler interpretable model, such as rule models like a decision set/list/tree. Often, this approximation is handled as standard supervised learning and the only difference is that the labels are provided by the target classifier instead of ground truth. This paradigm is particularly popular because there exists a variety of well-studied supervised algorithms for learning an interpretable classifier.

However, we argue that this paradigm is suboptimal for it does not utilize the unique property of the model interpretation problem, that is, the ability to generate synthetic instances and query the target classifier for their labels. We call this the active-query property, suggesting that we should consider model interpretation from an active learning perspective. Following this insight, we argue that the active-query property should be employed when designing a model interpretation algorithm, and that the generation of synthetic instances should be integrated seamlessly with the algorithm that learns the model interpretation. In this paper, we demonstrate that by doing so, it is possible to achieve more faithful interpretation with simpler model complexity. As a technical contribution, we present an active algorithm Active Decision Set Induction (ADS) to learn a decision set, a set of if-else rules, for model interpretation. ADS performs a local search over the space of all decision sets. In every iteration, ADS computes confidence intervals for the value of the objective function of all local actions and utilizes active-query to determine the best one to apply.

2 Related work

We discuss global model interpretation methods that approximate the global behavior of a target classifier and we further restrict ourselves to rule-based methods.

First introduced is the mainstream of model interpretation methods which we refer to as passive methods, in the sense that it approximates a fixed-sized dataset labelled by the target classifier, rather than the target classifier itself. Lakkaraju et al. (2017, 2019) learns a decision set for model interpretation by jointly optimizing interpretability and approximation faithfulness on the relabelled dataset. Following this widely-cited approach, a variety of alternative algorithms for learning an interpretable classifier (Lakkaraju et al., 2016; Wang et al., 2017; Yang et al., 2017) can be applied in the context of model interpretation. But the problem is that the given dataset, in practice, may not be good enough to reveal the true decision boundary of the target classifier and and thus whether this interpretable simpler model can faithfully approximate the target classifier is in question. The approaches of Ming et al. (2018); Paçaci et al. (2019); Sushil et al. (2018) first augment the dataset and then apply the main algorithm for learning an interpretable model. For example, Ming et al. (2018) first estimate the data distribution and then sample an arbitrarily large dataset. Passive methods can utilize new data instances, but only as preprocessing which is separate from the main learning algorithm, and thus we argue is suboptimal.
Another line of work, which we call bottom-up methods, applies two-phase local-to-global algorithms (Pedreschi et al., 2018) leveraging the relatively well-studied local interpretation methods (Ribeiro et al., 2016, 2018; Guidotti et al., 2018). The idea is to first construct a local interpretation for each instance in the dataset, and then select a subset of them to produce a global interpretation.

Lastly, we introduce the work closest to ours, DT-Extract (Bastani et al., 2017), as it integrates active-query seamlessly into the algorithm. It modifies the classic decision tree algorithm CART by generating new instances at each node to select the best split and thus better approximates the target classifier. We believe this tree-growing approach has been re-invented many times (Bastani et al., 2017; Craven, 1996; Breiman and Shang, 1996) though in different contexts and suffers from the inherent drawback of decision tree methods, that its approximation does not consider interpretability explicitly. In order to be interpretable, the number of node splits is hard-coded and thus the number of leaf nodes is controlled. We refer to these methods as top-down methods.

3 Definitions and Problem Formulation

We are given a pre-trained binary classifier \( f \) that receives an instance \( x \) and returns a prediction \( f(x) \in \{0, 1\} \). Let \( X = \{x\}^n = \{(a_1, a_2, ..., a_m)\}^n \) represent an instance set of \( n \) instances with \( m \) attributes. The input space is defined as \( D_x = \{dom(a_i)\}^m \). The form of model interpretation is a decision set, consisting of a set of if-then rules. It predicts the positive class if at least one of the rules is satisfied and predicts the negative class otherwise. A condition (clause) \( c \) consists of an attribute and a range of values this attribute can take. Conditions on continuous attributes are specified as bounded intervals, for example, ‘price’ \( \in [2.33, 10) \), and conditions on categorical features as a list of values, for example, ‘state’ \( \in \{\text{California, Texas}\} \). A rule is a conjunction of conditions \( r = c_1 \land c_2 \land ... \land c_r \). We use \( r(\cdot) \) to represent the Boolean function \( r(\cdot) : D_x \rightarrow \{0, 1\} \), which computes whether or not an instance \( x \) satisfies \( r \).

**Definition 1.** A decision set is a set of rules, denoted as \( S = \{r_1, r_2, ...\} \). An instance is predicted as positive if it satisfies at least one of the rules, as defined by \( S(\cdot) : S(x) = \begin{cases} 1 & \text{if } \exists r \in S, r(x) = 1 \\ 0 & \text{otherwise.} \end{cases} \)

Our goal is to determine a decision set \( S \) that maximizes a simple objective function

\[
Q(S) = \theta_S - \lambda|S|
\]

where the first term \( \theta_S = E_{x \sim P(X)}[\mathbb{1}_{f(x) = S(x)}] \) measures the faithfulness of the approximation of our decision set to the target classifier, defined as the expected accuracy over the input space. \(|S|\) denotes the number of rules in \( S \) as a measure of interpretability. \( \lambda \) is a tunable hyper-parameter set to 0.01 by default, meaning that a 1% accuracy improvement is worth adding an extra rule.

**Remark.** The design of the objective function is not the focus of this paper. Any reasonable objective could be used instead, such as Lakkaraju et al. (2016, 2019); Wang et al. (2017), as interpretability comes in different forms in different domains (Freitas, 2014; Huysmans et al., 2011).

4 Active Decision Set Induction for model interpretation

Given a target classifier \( f \) and a data set of real data instances \( X \), our goal is to find a decision set that maximizes the objective function \( Q \). We propose a local search algorithm called Active Decision Set Induction (ADS) which utilizes active query to determine the best action in each iteration. The decision set \( S \) is initialized as empty. In each iteration, a set of actions \( \mathcal{A} \) that locally modify the current decision set is generated, among which the best action \( a \in \mathcal{A} \) is determined and then applied to maximize \( Q \). The actions considered at each iteration are modifications of the current decision set of the following types, adding/removing a rule, adding/removing/modifying a condition of a rule. After actions are generated, active query is utilized to determine the increase of objective function after applying an action. To escape from local optima, a simple \( \epsilon \)-greedy strategy is employed: with probability \( \epsilon \), the algorithm chooses a random action.

**When to utilize active query?** In the framework of local search, the best action for maximizing the objective is chosen and applied. For the problem of model interpretation, it is non-trivial to determine the best action, because the faithfulness term \( \theta_S = E_{x \sim P(X)}[\mathbb{1}_{f(x) = a(S)(x)}] \) (the first term of \( Q \)) can only be estimated as \( \hat{\theta}_S = E_{x \in X \cup X'}[\mathbb{1}_{f(x) = a(S)(x)}] \), where \( X' \) is a set of generated
INPUT: A tuple \((Q, f, X)\), \(Q\) - the objective function, \(f\) - the target classifier model, \(X\) - the given set of instances

Algorithm Parameters: \(\beta\) - the confidence parameter, \(\epsilon\) - the randomness for \(\epsilon\)-greedy strategy, \(N_{max}\) - the maximum number of iteration for the local search

OUTPUT: \(S\) - the decision set

1: procedure MAIN
2: \(S_0 \leftarrow \emptyset\) \(\triangleright\) initialize an empty decision set
3: \(Y \leftarrow f(X)\) \(\triangleright\) query existed data instances
4: \(X' \leftarrow \emptyset, Y' \leftarrow \emptyset\) \(\triangleright\) an empty set of synthetic instances
5: for \(t = 1, 2, \ldots, N_{max}\) do
6: \(A \leftarrow \text{GenerateActions}(S_{t-1})\) \(\triangleright\) Add/remove a rule, etc
7: \(a^* \leftarrow \text{argmax}_{a \in A} \hat{Q}(a(S_{t-1}))\)
8: \(a' \leftarrow \text{argmax}_{a \in A, a \neq a^*} U_a\)
9: while \(L_{a^*} < U_{a'}\) do
10: \(x_1 \leftarrow \text{GenerateSyntheticInstances}(r_{a^*}, X); y_1 \leftarrow f(x_1)\)
11: \(x_2 \leftarrow \text{GenerateSyntheticInstances}(r_{a'}, X); y_2 \leftarrow f(x_2)\) \(\triangleright\) synthetic instances
12: \(X' \leftarrow X' \cup \{x_1, x_2\}, Y' \leftarrow Y' \cup \{y_1, y_2\}\)
13: update \(\hat{Q}(\{S_{t-1}\})\) and \(\bar{Q}(a'(S_{t-1}))\)
14: \(a^* \leftarrow \text{argmax}_{a \in A} \hat{Q}(a(S_{t-1}))\)
15: \(a' \leftarrow \text{argmax}_{a \in A, a \neq a^*} U_a\) \(\triangleright\) reset \(a^*\) and \(a'\)
16: end while
17: \(S_{max} \leftarrow \max(\hat{Q}(a^*), \bar{Q}(S_{max}))\)
18: \(S_t = \{\text{a_random}(S_{t-1})\} \text{ with probability } \epsilon\)
19: \(\{a^*(S_{t-1})\} \text{ otherwise.}\)
20: return \(S_{max}\)
21: end procedure

Algorithm 1: The ADS algorithm

synthetic instances. It is, at this point of time, for determining the best action that active query is utilized. We borrow ideas from the best arm identification problem for pure-exploration bandits (Audibert and Bubeck, 2010; Kalyanakrishnan et al., 2012; Kaufmann and Kalyanakrishnan, 2013), particularly LUCB(Kalyanakrishnan et al., 2012). Note that since the rules of \(S\) are descriptive, we can use the rules to generate new instances and query the classifier to better estimate \(\theta_\alpha\), and thus determine the best action. For estimating \(\bar{Q}\) after applying an action \(a\) on the current decision set \(S\), a confidence interval is computed to construct a lower and an upper bound for \(\bar{Q}\). For some exploration rate \(\beta\), the lower bound and upper bound for an action \(a\) are computed as:

\[
L_a = \hat{Q}(a(S)) - \beta \sqrt{\frac{\rho_0}{\rho(r_a)}}, U_a = \hat{Q}(a(S)) + \beta \sqrt{\frac{\rho_0}{\rho(r_a)}},
\]

\(\beta\) is a hyper-parameter that controls the confidence level, and \(\rho(r_a) = \frac{N(r_a)}{V(r_a)}\) defines the relative density: \(r_a\) is the rule that is added, removed or modified by action \(a\), \(N(r_a)\) denotes the number of instances covered by this rule \(N(r_a) = |\{x|r_a(x) = 1\}|\) and \(V(r_a)\) denotes the volume of input space covered by \(r_a\), \(\rho_0\) is the pre-computed density of the given dataset over the entire input space.

Utilizing active-query exhaustively for each local action is possible, but the total number of actions can be very large, not to mention that we have to do it for each iteration. Therefore, we use an adaptive sampling scheme (Kaufmann and Kalyanakrishnan, 2013) focusing on only two well-chosen candidate actions: 1) the empirically best action that has the highest empirical estimate \(a^* \leftarrow \text{argmax}_{a \in A} \hat{Q}(a(S))\) and 2) the most optimistic action that has the highest upper bound \(a' \leftarrow \text{argmax}_{a \in A, a \neq a^*} U_a\). New instances are generated and queried to update the estimate and the bounds of the objective function for these two candidate actions. This process continues until the lower
bound of \(a^*\) is higher than the upper bound of \(a'\), i.e., \(L_{a^*} > U_{a'}\). If this termination condition is met, then we are confident that \(a^*\) is the best action among all other actions \(a \in A\) under the exploration rate \(\beta\). \(a^*\) is then applied, i.e., \(S\) is replaced by \(a^*(S)\) and the next iteration is started.

**Remark.** When \(\beta = 0\), no synthetic instances will be generated and queried as the termination condition will be immediately met. ADS then reduces to a passive approximation.

**How to generate instances for active query?** The descriptive nature of rules gives us an opportunity to generate new instances to query in order to refine the estimate of the value of the objective function after applying an action. In order to distinguish \(Q(a^*(S))\) and \(Q(a'(S))\) to determine the best action, at each round, one synthetic instance is generated for both \(a^*\) and \(a'\), and their labels are obtained by querying the classifier \(f\). The generation of new instances is formulated as pool-based sampling: we first generate a pool of candidate instances and then select one to label. For generating a pool of synthetic instances as candidates for action \(a\), note that the alternative actions considered at an iteration have only an edit distance of 1 from \(S\), we focus on \(r_a\), the rule modified by \(a\). A pool of instances \(X_{pool} = \{x \mid r_a(x) = 1\}\) is randomly generated.

We devise a simple pool-generation scheme called Counterfactual Sampling to generate the random pool \(X_{pool}\). We randomly pick instances from \(\{x \mid x \in X \cup X', r_a(x) = 0\}\) and modify them to satisfy \(r_a(x) = 1\). Instances are modified to satisfy \(r_a\) by replacing the value of the specified attributes by the condition of \(r_a\) with uniform-randomly sampled values. For example, given \(r_a = \{\text{’price’} \in [2.33, 10]\}\) specified on the ’price’ attribute and a data instance \(x = \{\text{’state’} = \text{’Texas’}, \text{’price’} = 1\}\) that \(r_a(x) = 0\), the modified instance \(x'\) will be \{’state’ = ’Texas’, ’price’ = 5\} where 5 is drawn uniformly from \([2.33, 10]\) and now \(r_a(x') = 1\). The rationale for this counterfactual sampling is as follows. To sample \(X_{pool}\), we first tried uniform randomness but it did not work well. Probably because the generated instances are not from the data distribution \(P(X)\). We also tried to first estimate \(P(X)\) and then perform rejection-sampling \(\{x \mid x \sim \hat{P}(X), r_a(x) = 1\}\), which improved the performance only slightly, perhaps because the quality of estimation of \(P(X)\) matters and estimating \(P(X)\) is already very hard. The proposed Counterfactual sampling avoids estimating the true data distribution \(P(X)\) and still works well to generate instances as \(f\) if they were from \(P(X)\).

For selecting an instance to label, one synthetic instance that maximizes the distance to its nearest neighbor among all existing instances satisfying \(r_a\) \(\{x \mid r_a(x) = 1, x \in X \cup X'\}\) is selected from the candidate pool. We then query \(f\) to get the label and append it to \(X'\) to refine \(Q(a(S))\).

**Remark.** While more sophisticated heuristics for uncertainty-based sampling exist (MacKay, 1992; Bryan et al., 2006), we choose to use the largest distance to its nearest neighbor as the sampling criteria, not only because most of the uncertainty measures are essentially based on it, but also we find that it works well and is computationally efficient.

### 5 Evaluation

We run experiments on the Income Census Prediction (Adult) dataset (Kohavi, 1996), for it is a widely-used and relatively large tabular dataset (48842 instances). We use a 90%-10% train-test split and train a 5-layer fully-connected Deep Neural Network on the training set. Model interpretation methods are also applied on the train set and evaluated on the test set.

We analyze the dependency of ADS from different choices of the hyper-parameters \(\lambda\) and \(\beta\). We run ADS for different values of \(\beta\) and report the curve of F1 score v.s. \(|S|\) in Figure 1. For a given value of \(\beta\), we vary \(\lambda\) to get different numbers of rules. Note that the exploration rate \(\beta\) controls the number of active queries: a larger \(\beta\) will use more active queries while \(\beta \leftarrow 0\) reduces ADS to passive mode without generating any synthetic instances. We find that as \(\beta\) gets larger, the curve moves towards the top-left corner, indicating that ADS can achieve better approximation with even fewer rules with the help of active query.

We then compare ADS with several baselines on various metrics for both faithfulness (F1 score, precision and recall) and interpretability (number of rules, number of conditions, etc). For baselines, we consider one representative method for each of three categories (passive, bottom-up, top-down) discussed in Related Work. For passive methods, we choose SBRL+ (Ming et al., 2018) which first enlarges the dataset and then learns a Scalable Bayesian Rule List (SBRL) (Yang et al., 2017). We replace SBRL with Bayesian Rule Set (BRS) (Wang et al., 2017) for a fair comparison and call this BRS+. For bottom-up methods that merge local interpretations into a global one, we choose SP-anchor (Ribeiro et al., 2018). As a representative of top-down active methods, DT-Extract (Bastani...
et al., 2017) is also compared. All root-to-leaf paths are extracted as decision rules from the tree. For SP-anchor and DT-Extract, since the number of rules can be controlled through hyper-parameters, we force them to produce the same number of rules as ADS. The result presented in Table 1 shows that ADS significantly outperforms the baselines in all faithfulness metrics (except precision) and in all interpretability metrics. Compared to ADS non active, ADS greatly improves the recall and F1-score. SP-anchor and DT-Extract produce rules of very high precision but surprisingly low recall, in some way failing the purpose of approximating the global behavior of the target classifier.

Figure 1: Tuning the parameter $\lambda$ and $\beta$

Table 1: comparison of ADS against baselines

5 Conclusion

In this paper, we present ADS, an active approach for model interpretation and demonstrate that integrating active-query into the algorithm is beneficial for finding better model interpretations, in terms of both faithfulness and interpretability. Though ADS is only a simple algorithm and needs further polishing, our preliminary experimental results suggest that the active-query paradigm is promising for designing advanced model interpretation algorithms, especially iteration-based discrete optimization algorithms.

limitations. The main limitations of ADS is that its algorithm still appears to be too weak in terms of optimality. The greedy hill-climbing does not ensure convergence and taking the greedy action sometimes may not give the best result. It might make more sense to identify the best action to apply considering a longer range of iterations. Second, because of the generated synthetic instances, the estimate of the objective function $Q$ is biased by the local search procedure and the given dataset. A clever way to solve this issue is desired. Last, the ADS method, as well as most of the related methods we discussed, do not consider the role of uncertainty which is indeed very crucial for model interpretation.
References

Jean-Yves Audibert and Sébastien Bubeck. 2010. Best arm identification in multi-armed bandits.

Osbert Bastani, Carolyn Kim, and Hamsa Bastani. 2017. Interpreting Blackbox Models via Model Extraction. CoRR abs/1705.08504 (2017). arXiv:1705.08504 http://arxiv.org/abs/1705.08504

Leo Breiman and Nong Shang. 1996. Born again trees. (1996).

Brent Bryan, Robert C. Nichol, Christopher R Genovese, Jeff Schneider, Christopher J. Miller, and Larry Wasserman. 2006. Active Learning For Identifying Function Threshold Boundaries. In Advances in Neural Information Processing Systems 18, Y. Weiss, B. Schölkopf, and J. C. Platt (Eds.). MIT Press, 163–170. http://papers.nips.cc/paper/2940-active-learning-for-identifying-function-threshold-boundaries.pdf

Mark William Craven. 1996. Extracting Comprehensible Models from Trained Neural Networks. Ph.D. Dissertation. AAI9700774.

Alex A. Freitas. 2014. Comprehensible classification models. ACM SIGKDD Explorations Newsletter 15, 1 (mar 2014), 1–10. https://doi.org/10.1145/2594473.2594475

Riccardo Guidotti, Anna Monreale, Salvatore Ruggieri, Dino Pedreschi, Franco Turini, and Fosca Giannotti. 2018. Local Rule-Based Explanations of Black Box Decision Systems. CoRR abs/1805.10820 (2018). arXiv:1805.10820 http://arxiv.org/abs/1805.10820

Johan Huysmans, Karel Dejaeger, Christophe Mues, Jan Vanthienen, and Bart Baesens. 2011. An empirical evaluation of the comprehensibility of decision table tree and rule based predictive models. Decision Support Systems 51, 1 (apr 2011), 141–154. https://doi.org/10.1016/j.dss.2010.12.003

Shivaram Kalyanakrishnan, Ambuj Tewari, Peter Auer, and Peter Stone. 2012. PAC Subset Selection in Stochastic Multi-armed Bandits. In ICML, Vol. 12. 655–662.

Emilie Kaufmann and Shivaram Kalyanakrishnan. 2013. Information complexity in bandit subset selection. In Conference on Learning Theory. 228–251.

Ron Kohavi. 1996. Scaling Up the Accuracy of Naive-Bayes Classifiers: A Decision-tree Hybrid. In Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD ’96). AAAI Press, 202–207. http://dl.acm.org/citation.cfm?id=3001460.3001502

Himabindu Lakkaraju, Stephen H. Bach, and Jure Leskovec. 2016. Interpretable Decision Sets: A Joint Framework for Description and Prediction. In Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD ’16). ACM, New York, NY, USA, 1675–1684. https://doi.org/10.1145/2939672.2939874

Himabindu Lakkaraju, Ece Kamar, Rich Caruana, and Jure Leskovec. 2017. Interpretable & Explorable Approximations of Black Box Models. CoRR abs/1707.01154 (2017). arXiv:1707.01154 http://arxiv.org/abs/1707.01154

Himabindu Lakkaraju, Ece Kamar, Rich Caruana, and Jure Leskovec. 2019. Faithful and Customizable Explanations of Black Box Models. AIES (2019).

David J. C. MacKay. 1992. Information-Based Objective Functions for Active Data Selection. Neural Computation 4, 4 (jul 1992), 590–604. https://doi.org/10.1162/neco.1992.4.4.590

Yao Ming, Huamin Qu, and Enrico Bertini. 2018. RuleMatrix: Visualizing and Understanding Classifiers with Rules. CoRR abs/1807.06228 (2018). arXiv:1807.06228 http://arxiv.org/abs/1807.06228

Görgem Paçaci, David Johnson, Steve McKeever, and Andreas Hamfelt. 2019. Why did you do that?: Explaining black box models with Inductive Synthesis. CoRR abs/1904.09273 (2019). arXiv:1904.09273 http://arxiv.org/abs/1904.09273
Dino Pedreschi, Fosca Giannotti, Riccardo Guidotti, Anna Monreale, Luca Pappalardo, Salvatore Ruggieri, and Franco Turini. 2018. Open the Black Box Data-Driven Explanation of Black Box Decision Systems. CoRR abs/1806.09936 (2018). arXiv:1806.09936 http://arxiv.org/abs/1806.09936

Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. Why Should I Trust You?. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD 16. ACM Press. https://doi.org/10.1145/2939672.2939778

Marco Túlio Ribeiro, Sameer Singh, and Carlos Guestrin. 2018. Anchors: High-Precision Model-Agnostic Explanations. In AAAI.

Madhumita Sushil, Simon Suster, and Walter Daelemans. 2018. Rule induction for global explanation of trained models. CoRR abs/1808.09744 (2018). arXiv:1808.09744 http://arxiv.org/abs/1808.09744

Tong Wang, Cynthia Rudin, Finale Doshi-Velez, Yimin Liu, Erica Klampfl, and Perry MacNeille. 2017. A Bayesian Framework for Learning Rule Sets for Interpretable Classification. Journal of Machine Learning Research 18, 70 (2017), 1–37. http://jmlr.org/papers/v18/16-003.html

Hongyu Yang, Cynthia Rudin, and Margo Seltzer. 2017. Scalable Bayesian Rule Lists. In Proceedings of the 34th International Conference on Machine Learning - Volume 70 (ICML’17). JMLR.org, 3921–3930. http://dl.acm.org/citation.cfm?id=3305890.3306086