The Solvability of Interpretability Evaluation Metrics

Yilun Zhou
MIT CSAIL
yilun@csail.mit.edu

Julie Shah
MIT CSAIL
julie_a_shah@csail.mit.edu

Abstract

Feature attribution methods are popular for explaining neural network predictions, and they are often evaluated on metrics such as comprehensiveness and sufficiency, which are motivated by the principle that more important features – as judged by the explanation – should have larger impacts on model prediction. In this paper, we highlight an intriguing property of these metrics: their *solvability*. Concretely, we can define the problem of optimizing an explanation for a metric and solve it using beam search. This brings up the obvious question: given such solvability, why do we still develop other explainers and then evaluate them on the metric? We present a series of investigations showing that this beam search explainer is generally comparable or favorable to current choices such as LIME and SHAP, suggest rethinking the goals of model interpretability, and identify several directions towards better evaluations of new method proposals.

1 Introduction

For neural network models deployed in high stakes domains, the explanations for predictions are often as important as the predictions themselves. For example, a skin cancer detection model may work by detecting surgery markers (Winkler et al., 2019) and an explanation that reveals this spurious correlation is highly valuable. However, evaluating the correctness (or faithfulness) of explanations is fundamentally ill-posed: because the explanations are used to help people understand the reasoning of the model, we cannot check it against the ground truth reasoning, as the latter is not available.

As a result, correctness evaluations typically employ proxy metrics. For feature attribution explanations, they work under a shared principle: changing an important feature should have a large impact on the model prediction. Thus, the quality of the explanation is defined by aspects of the model prediction change, such as comprehensiveness and sufficiency (DeYoung et al., 2020). To develop new explanation methods (Fig. 1, left), people generally identify a specific notion of feature importance (e.g. local sensitivity), propose the corresponding explainer (e.g. gradient saliency (Simonyan et al., 2014)), evaluate it on one or more metrics, and claim its superiority based on favorable results vs. baseline explainers. As they are motivated by notions of feature importance, we call them *heuristic explainers*.

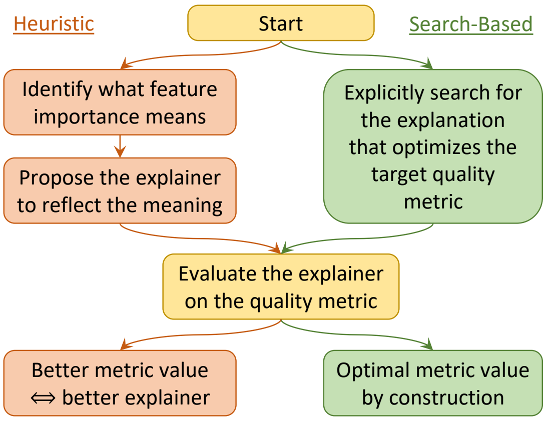

Heuristic
Start
Search-Based
Identify what feature importance means
Propose the explainer to reflect the meaning
Explicitly search for the explanation that optimizes the target quality metric
Evaluate the explainer on the quality metric
Better metric value ⟺ better explainer
Optimal metric value by construction

Figure 1: Left: the current process of developing new explainers. Right: the natural implication following our observation that evaluation metrics are *solvable*.

In this paper, we show that all these metrics are *solvable*, in that we can *define* an explanation as the one that optimizes a metric value and *search* for it. The elephant-in-the-room question is then: *if we take a specific target metric to represent correctness, why don't we just search for the metric-optimal explanation (Fig. 1, right) but take the more convoluted route of developing heuristic explanations and then evaluating them (Fig. 1, left)?*

There are several possible reasons. First, the optimization problem may be so hard that we cannot find an explanation better than the heuristic ones. The bigger concern, however, is that of the Goodhart's Law. In other words, as soon as a metric is used in explicit optimization, it ceases to be a good metric. Concretely, the explanation may overfit to the particular metric and perform much worse on closely related ones (Chan et al., 2022), or overfit to the model and effectively adversarially attack the model when assigning word importance (Feng et al., 2018). It may also perform poorly on evaluations not based on proxy metrics, such as ground truth alignment (Zhou et al., 2022a).

We assess these concerns, taking the widely used comprehensiveness and sufficiency metrics (DeYoung et al., 2020) as the optimization target. Our findings, however, largely dispel every concern. A standard beam search produces explanations that greatly outperform existing one such as LIME and SHAP on the target metric. On several other metrics, the search-based explainer also performs favorably on average. There is no strong evidence of it adversarially exploiting the model either. Last, it achieves competitive performances on a suite of ground truth-based evaluations.

Hence, we argue that we should rethink the development of novel explainers. First, the search-based explainer should be considered as a strong baseline. In addition, Sec. 6 presents the lack of privileged information as the fundamental reason for metric solvability: the beam searcher knows exactly how to produce an (approximately) optimal solution. This loophole is fixed in the ground truth-based evaluations. Finally, we advocate for evaluations that can demonstrate concrete utilities of explanations in real-world scenarios.

2 Background and Related Work

In this section, we give a concise but unified introduction to the popular feature attribution explainers and evaluation metrics studied in this paper.

2.1 Feature Attribution Explainers

We focus on feature attribution explanations, which explains an input $x = (x_1, ..., x_L)$ by a vector $e = (e_1, ..., e_L)$ where e_l represents the "contribution" of x_l to the prediction. Many different definitions for contribution have been proposed and we consider the following five.

- **Vanilla gradient (Grad)** (Simonyan et al., 2014; Li et al., 2016a) is the L2 norm of gradient of the prediction (in logit, following standard practice) with respect to the token embedding.
- **Integrated gradient (IntG)** (Sundararajan et al., 2017) is the path integral of the embedding gradient along the line segment between the zero embedding value and the actual value.
- **LIME** (Ribeiro et al., 2016) is the coefficient of a linear regression in the local neighborhood.
- **SHAP** (Lundberg and Lee, 2017) computes the Shapley value (Roth, 1988) for each word.
- **Occlusion (Occl)** (Li et al., 2016b) is the change in prediction when a word is removed from the input while all other words remain.

2.2 Feature Attribution Evaluations

Naturally, different definitions of contribution result in different explanation values. As findings (e.g. Adebayo et al., 2018; Nie et al., 2018) suggest that some explanations are not correct (i.e. faithfully reflecting the model's reasoning process), many evaluations are proposed to quantify the correctness of different explanations. Not having access to the ground truth model working mechanism (which is what explanations seek to reveal in the first place), they are instead guided by one principle: changing an important feature (according to the explanation) should have a large impact on the prediction, and the impact size is taken as explanation quality. However, there are different ways to quantify the impact, leading to different evaluations, and we consider six in this paper.

Let $f : \mathcal{X} \to \mathbb{R}$ be the function to compute model prediction. We define it as the scalar function, such as the probability for the predicted class. For an input $x = (x_1, ..., x_L)$ of L words and a feature explanation e, we can create a sequence of $L + 1$ input deletions $\tilde{x}^{(0)}, \tilde{x}^{(1)}, ..., \tilde{x}^{(L)}$ where that $\tilde{x}^{(l)}$ is the the input but with l most important features removed. Thus, we have $\tilde{x}^{(0)} = x$ and $\tilde{x}^{(L)}$ being the empty string. The **comprehensiveness** κ (DeYoung et al., 2020) is defined as

$$\kappa(x, e) = \frac{1}{L+1} \sum_{l=0}^{L} f(x) - f(\tilde{x}^{(l)}). \qquad (1)$$

It measures the deviation from the original model prediction when important features (according to e) are successively removed, and therefore a larger value is desirable. It was also proposed earlier for computer vision models as the area over perturbation curve (AoPC) by Samek et al. (2016).

Analogously, we can define the sequence of input insertions $\widehat{x}^{(0)}, \widehat{x}^{(1)}, ..., \widehat{x}^{(L)}$, where $\widehat{x}^{(l)}$ is the input with the l most important features present. Thus, $\widehat{x}^{(0)}$ is the empty string and $\widehat{x}^{(L)} = x$, but otherwise the sequences of input insertions and deletions do not mirror each other. The **sufficiency** σ (DeYoung et al., 2020) is defined as

$$\sigma(x, e) = \frac{1}{L+1} \sum_{l=0}^{L} f(x) - f(\widehat{x}^{(l)}). \qquad (2)$$

It measures the gap to the original model prediction that remains (i.e. convergence to the model prediction) when features are successively inserted from the most important to the least. Therefore, a smaller value is desirable.

Another interpretation of prediction change just considers decision flips. Let $g : \mathcal{X} \to \{0, ..., K\}$ be the function that outputs the most likely class of an input. The **decision flip by removing the most important token** (Chrysostomou and Aletras, 2021) is defined as

$$\mathrm{DF}_{\mathrm{MIT}}(x, e) = \mathbb{1}_{g(\tilde{x}^{(1)}) \neq g(x)}, \tag{3}$$

which measures whether removing the most important token changes the decision. Across a dataset, its average value gives the overall decision flip rate, and a higher value is desirable.

The **fraction of token removals for decision flip** (Serrano and Smith, 2019) is defined as

$$\mathrm{DF}_{\mathrm{Frac}}(x, e) = \frac{\arg\min_l g(\tilde{x}^{(l)}) \neq g(x)}{L}, \tag{4}$$

and we define $\mathrm{DF}_{\mathrm{Frac}} = 1$ if no value of l leads to the decision flip. This metric represents the fraction of feature removals that is needed to flip the decision, and hence a lower value is desirable.

Last, two metrics evaluate correlations between model prediction and feature importance. For an input x and explanation e, we define the sequence of marginal feature deletions $x_{-}^{(1)}, ..., x_{-}^{(L)}$ such that $x_{-}^{(l)}$ is original input with only the l-th important feature removed. The **deletion rank correlation** (Alvarez-Melis and Jaakkola, 2018) is defined as

$$\delta_f = [f(x) - f(x_{-}^{(1)}), ..., f(x) - f(x_{-}^{(L)})], \tag{5}$$

$$\mathrm{Rank}_{\mathrm{Del}}(x, e) = \rho(\delta_f, e), \tag{6}$$

where $\rho(\cdot, \cdot)$ is the Spearman rank correlation coefficient between the two input vectors. Intuitively, this metric asserts that suppressing a more important feature should have a larger impact to the model prediction. A higher correlation is desirable.

The **insertion rank correlation** (Luss et al., 2021) is defined as

$$v = [f(\tilde{x}^{(L)}), ..., f(\tilde{x}^{(0)})], \tag{7}$$

$$\mathrm{Rank}_{\mathrm{Ins}}(x, e) = \rho(v, [0, ..., L]), \tag{8}$$

and recall that $\tilde{x}^{(L)}, ..., \tilde{x}^{(0)}$ is the sequence of inputs with increasingly more important features inserted, starting from the empty string $\tilde{x}^{(L)}$ to the full input $\tilde{x}^{(0)}$. This metric asserts that the model prediction on this sequence should increase monotonically to the original prediction. Also a higher correlation is desirable.

3 The Solvability of Evaluation Metrics

Now we establish the central observation of this paper: the solvability of these evaluation metrics. Observe that each evaluation metric, e.g. comprehensiveness κ, is defined on the input x and the explanation e, and its computation only uses the model prediction function f (or g derived from f for the two decision flip metrics). In addition, the form of feature attribution explanation constrains e to be a vector of the same length as x, or $e \in \mathbb{R}^L$.

Without loss of generality, we assume that the metrics are defined such that a higher value means a better explanation (e.g. redefining the sufficiency to be the negative of its original form). We formalize the concept of solvability as follows:

Definition 3.1. For a metric m and an input x, an explanation e^* *solves* the metric m if $m(x, e^*) \geq m(x, e)$ for all $e \in \mathbb{R}^L$. We also call e^* the m-*solving* explanation.

Notably, there are already two explanation-solving-metric cases among the ones in Sec. 2.

Theorem 1. The occlusion explainer solves the $\mathrm{DF}_{\mathrm{MIT}}$ and $\mathrm{Rank}_{\mathrm{Del}}$ metrics.

The proof follows from the definition of the explainer and the two metrics. Occlusion explainer defines token importance as the prediction change when each the token is individually removed, thus the most important token is the one that induces the largest change, which makes it most likely to flip the decision under $\mathrm{DF}_{\mathrm{MIT}}$. In addition, because token importance is defined as the model prediction change, its rank correlation with the latter (i.e. $\mathrm{Rank}_{\mathrm{Del}}$) is maximal at 1.0.

Thm. 1 highlights an important question: if we take $\mathrm{DF}_{\mathrm{MIT}}$ or $\mathrm{Rank}_{\mathrm{Del}}$ as the metric (i.e. indicator) of explanation quality, why should we consider any other explanation, when the occlusion explanation provably achieves the optimum? A possible answer is that the metrics themselves are problematic. For example, one can argue that the $\mathrm{DF}_{\mathrm{MIT}}$ is too restrictive for overdetermined input: when redundant features (e.g. synonyms) are present, removing any individual one cannot change the prediction, such as for the sentiment classification input of “This movie is great, superb and beautiful.”

Nonetheless, the perceived quality of a metric can be loosely inferred from its adoption by the community, and the comprehensiveness and sufficiency metrics (DeYoung et al., 2020) are by far the most widely used. They overcome the issue of

DF$_{\text{MIT}}$ by also considering inputs with more than one token removed. Since a metric value is scalar, we combine comprehensiveness κ and sufficiency σ into comp-suff difference Δ, defined as (recall that a *lower* sufficiency value is better):

$$\Delta(x, e) = \kappa(x, e) - \sigma(x, e). \tag{9}$$

Again, we face the same question: if Δ is solvable, why should *any* heuristic explainers be used instead of the Δ-solving e^*? In the next two sections, we seek to answer it by first proposing a beam search algorithm to (approximately) find e^* and then explore its various properties.

4 Solving Metrics with Beam Search

We first define two properties – value agnosticity and additivity – satisfied by some metrics.

Definition 4.1. For an input $x = (x_1, ..., x_L)$ with explanation $e = (e_1, ..., e_L)$, we define the ranked importance as $r(x_l) = |\{e_i : e_i \leq e_l, 1 \leq i \leq L\}|$. In other word, the x_l with $r(x_l) = L$ is the most important, and that with $r(x_l) = 1$ is the least. A metric m is *value-agnostic* if for all e_1 and e_2 that induce the same ranked importance, we have

$$m(x, e_1) = m(x, e_2). \tag{10}$$

A value-agnostic metric has at most $L!$ unique values across all possible explanations for an input of length L. Thus, in theory, an exhaustive search over the $L!$ permutations of the list $[1, 2, ..., L]$ is guaranteed to find the e^* that solves the metric.

Definition 4.2. A metric m is *additive* if it can be written in the form of

$$m(x, e) = \sum_{l=0}^{L} h(x, e^{(l)}), \tag{11}$$

for some function h, where $e^{(l)}$ reveals the attribution values of l most important features according to e but keeps the rest inaccessible.

Theorem 2. Comprehensiveness, sufficiency and their difference are value-agnostic and additive.

The proof is straightforward, by observing that both $\tilde{x}^{(l)}$ and $\widehat{x}^{(l)}$ can be created from x and the ordering of $e^{(l)}$. In fact, all metrics in Sec. 2 are value-agnostic (but only some are additive).

A metric satisfying these two properties admits an efficient beam search algorithm to approximately solve it. As $e^{(l)}$ can be considered as a partial explanation that only specifies the top-l important features, we start with $e^{(0)}$, and attempt each feature to extend to obtain $e^{(1)}$. With beam size B, if there are more than B features, we keep the top-B according to the partial sum. This extension procedure continues until all features are added, and top extension is then e^*. Alg. 1 documents the procedure, where $\text{extend}(e, v)$ creates a set of explanations in which each element has a value of v in a previously empty location of e.

Algorithm 1: Beam search for finding e^*.

```
Input: beam size $B$, metric $m$, sentence $x$
  of length $L$;
Let $e^{(0)}$ be an empty length-$L$ explanation;
$\texttt{beam} \leftarrow \{e^{(0)}\}$;
for $l = 1, ..., L$ do
    $\texttt{beam} \leftarrow \bigcup_{e \in \texttt{beam}} \text{extend}(e, L - l + 1)$;
    $\texttt{beam} \leftarrow \text{choose\_best}(\texttt{beam}, B)$;
end
return $\text{choose\_best}(\texttt{beam}, 1)$;
```

Without the additive property, beam search is not feasible due to the lack of partial metric values. However, Zhou et al. (2021) presented a simulated annealing algorithm (Kirkpatrick et al., 1983) to search for the optimal data acquisition order in active learning, and we can use a similar procedure to search for the optimal feature importance order. If the metric is value-sensitive, assuming that it is continuous and differentiable with respect to the explanation value, we can use techniques such as gradient descent to search for e^*. Since we focus on comprehensiveness and sufficiency in this paper, the development and evaluation of these approaches are left to future work.

5 Experiments

We investigate various properties of the beam search explainer vs. existing heuristic explainers, using the publicly available textattack/roberta-base-SST-2 model on the SST dataset (Socher et al., 2013) as a case study. The sentiment value for each sentence is a number between 0 (very negative) and 1 (very positive), which we binarize into two classes of $[0, 0.4]$ and $[0.6, 1]$. Sentences with sentiment values in middle are discarded. The average sentence length is 19, making the exhaustive search impossible. We use a beam size of 100 to search for Δ-solving explanation E*. All reported statistics are computed on the test set.

5.1 Qualitative Inspection

Fig. 2 presents two explanations, with additional ones in Fig. 6 of App. A. While we need more quantitative analyses (carried out below) for definitive conclusions on its various properties, E* explanations at least looks reasonable and could plausibly help people understand the model.

A worthy tribute to a great humanitarian and her vibrant ‘ co-stars . ’

So stupid , so ill-conceived , so badly drawn , it created whole new levels of ugly .

Figure 2: Two E* explanations. The shade of background color represents feature importance.

5.2 Performance on the Target Metric

We compare E* to heuristic explainers on the Δ metric, with results shown in Tab. 1 along with the associated κ and σ. A random explanation baseline is included for reference. We can see that E* achieves the best Δ, often by a large margin. It also tops the ranking separately for κ and σ, which suggests that an explanation could be optimally comprehensive and sufficient at the same time.

Explainer	Comp $\kappa\uparrow$	Suff $\sigma\downarrow$	Diff $\Delta\uparrow$
Grad	0.327	0.108	0.218
IntG	0.525	0.044	0.481
LIME	0.682	0.033	0.649
SHAP	0.612	0.034	0.578
Occl	0.509	0.040	0.469
E*	0.740	0.020	0.720
Random	0.218	0.212	0.006

Table 1: Comprehensiveness, sufficiency and their difference for various explainers.

To get a visual understanding about how the model prediction changes during feature removal and insertion, we plot in Fig. 3 the values of $f(x) - f(\tilde{x}^{(l)})$ and $f(x) - f(\widehat{x}^{(l)})$ (i.e. the summands in Eq. 1 and 2), as a function of l/L. The left panel shows the curves averaged across all test set instances, and the right panel shows those for a specific instance. κ and σ are thus the areas under the solid and dashed curves respectively. We can see that the curves for E* dominate the rest, and, on individual inputs, are also much smoother than those for other explanations.

Admittedly, beam search is slower than most other explainers, especially those that only require a single pass of the model such as the vanilla gradient. However, we note that explanations, unlike model predictions, are rarely used in real-time decision making. Instead, they are mostly used for debugging and auditing purposes, and incurring a longer generation time to obtain a higher-quality explanation is often beneficial. On a single RTX3080 GPU card without any in-depth code optimization, the metric values and time costs for various beam sizes are presented in Tab. 2, with statistics for the best explainer LIME also listed for comparison.

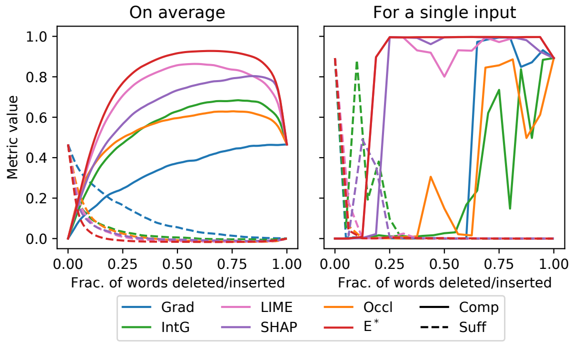


Figure 3: Comprehensiveness and sufficiency curves for the beam search optimal explainer vs. others.

B	1	5	10	20	50	100	LIME
κ	0.717	0.731	0.734	0.736	0.739	0.740	0.682
σ	0.020	0.020	0.020	0.020	0.020	0.020	0.033
Δ	0.697	0.711	0.714	0.716	0.719	0.720	0.649
T	0.56	2.15	4.53	8.83	21.01	41.00	4.75

Table 2: Effect of beam size B on metric values κ, σ, Δ and computation time T (in seconds), compared against the statistics of the best heuristic explainer LIME.

We have two observations. First, the metric values increase with increasing beam size, but the improvement is meager after 10 beams. Second, even the greedy search with a single beam outperforms LIME by a decent margin, while being almost 10 times faster. Thus, these results establish that *if we take comprehensiveness and sufficiency as the quality metrics*, there is really no reason not to use beam search directly as the explainer.

5.3 Performance on Other Metrics

Sec. 2 lists many metrics that all operationalize the same principle that changing important features should have large impact on model prediction, but in different ways. A potential argument against the explicit beam search optimization is the fulfillment of the Goodhart's Law: E* overfits to the metric by exploiting its realization (i.e. Eq. 1 and 2) of this principle and not truly reflecting its “spirit.”

To establish the legitimacy of this opposition, we evaluate all the explainers on the remaining four metrics in Sec. 2, and present the results in Tab. 3.

Since the occlusion explainer solves DF_{MIT} and Rank_{Del} (Thm. 1), it ranks the best on these two metrics, as expected. Nonetheless, E* still ranks

Explainer	$\text{DF}_{\text{MIT}}\uparrow$	$\text{DF}_{\text{Frac}}\downarrow$	$\text{Rank}_{\text{Del}}\uparrow$	$\text{Rank}_{\text{Ins}}\uparrow$
Grad	10.5%	54.5%	0.162	0.521
IntG	16.9%	39.6%	0.369	0.468
LIME	25.5%	28.1%	0.527	0.342
SHAP	23.0%	36.1%	0.369	0.458
Occl	26.4%	40.6%	1.000	0.396
E*	25.0%	25.2%	0.438	0.423
Random	3.4%	72.3%	0.004	0.599

Table 3: Performance on non-target metrics of the beam search optimal explainer vs. others.

competitively on these two metrics and comes out ahead on DF_{Frac}. The only exception is Rank_{Ins}, on which the random explanation surprisingly performs the best. We carefully analyze it in App. B and identify a fundamental flaw in it.

Last, note that we can also incorporate any of these metrics into the objective function(which already contains two metrics: κ and σ), and search for E* that performs overall the best, if so desired. We leave this investigation to future work.

5.4 Explainer "Attacking" the Model

Another concern is that the search procedure may overfit to the model. Specifically, removing a word w in a partial sentence $\tilde{x}^{(l)}$ drastically changes the model prediction but does not have the same effect for most other $\tilde{x}^{(l')}$. This makes E* assign w an overly high attribution, as w only happens to have a high impact in one particular case. By contrast, explainers like LIME and SHAP automatically avoid this issue by computing the average contribution of w on many different partial sentences.

We test this concern by locally perturbing the explanation. If E* uses many such "adversarial attacks," we should expect its metric values to degrade sharply under perturbation, as the high-importance words (according to E*) will no longer be influential in different partial sentence contexts.

To perturb the explanation, we first convert the each explanation e to its ranked importance version e_r using $r(\cdot)$ in Def. 4.1, which does not affect any metric as they are value-agnostic. Then we define the perturbed rank by adding to each entry of e_r an independent Gaussian noise: $e_r' = e_r + n$ with $n \sim \mathcal{N}(\mathbf{0}, s^2)$. Thus, two words x_i and x_j with $r(x_i) > r(x_j)$ have their ordering switched if the $r(x_i) - r(x_j) < n(x_j) - n(x_i)$. A visualization of the switching with different s is in Fig. 7 of App. C.

Fig. 4 plots the metrics under different s values (Rank_{Ins} not shown due to its intrinsic issue discussed in App. B). Everything degrades to various extents. Although E* degrades slightly faster than the rest on κ and DF_{Frac} (and on par on others), it still achieves best results even at $s = 4$, with many order switchings (Fig. 7), and a faster degradation is reasonable anyway for metrics with better starting values (c.f. occlusion on Rank_{Del}).

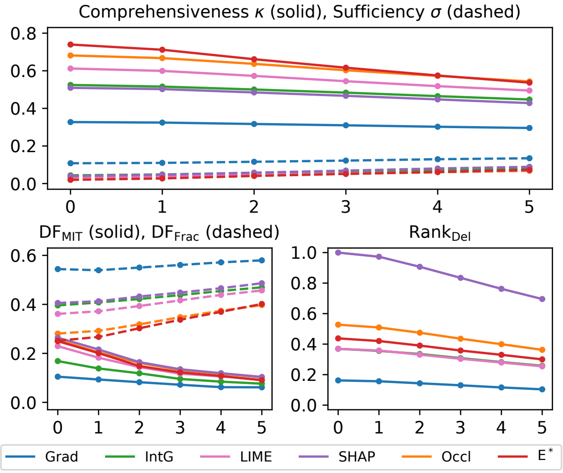


Figure 4: Metric values for explanations under different levels of perturbation represented by s on the x-axis.

The evidence suggests that there is at most a slight model overfitting phenomenon, as E* remains comparable to other explainers under quite severe perturbation. Furthermore, we can incorporate perturbation robustness into metric solving to obtain an E* that degrade less, similar to adversarial training (Madry et al., 2018). We leave the exploration of this idea to future work.

App. D describes another assessment of model overfitting, though with a mild assumption and relying on word-level sentiment scores provided by the SST dataset. Similar conclusions are reached.

5.5 Ground Truth Recovery

For a model trained on a natural dataset, its ground truth working mechanism is rarely available – in fact, it could be argued that the very purpose of interpretability methods is to uncover it. Thus, a series of work (Adebayo et al., 2020; Bastings et al., 2021; Zhou et al., 2022a) proposed methods to modify the dataset such that a model trained on the new dataset has to follow a certain working mechanism to achieve high performance, which allows for evaluations against the known mechanism.

Ground Truth Definitions We construct three types of ground truth features – short additions, long additions and replacements. First, we randomize the label to $\widehat{y} \sim \text{Unif}\{0, 1\}$ so that the original input features are no longer predictive, following the advice by Zhou et al. (2022a).

For the two addition types, a word or a sentence is inserted randomly to either the beginning or the end of the input. The inserted text is randomly chosen from the the corresponding set in Tab. 4.

Type	$\widehat{y} = 0$	$\widehat{y} = 1$
Short	terrible, awful, disaster, worst, never	excellent, great, fantastic, brilliant, enjoyable
Long	A total waste of time. Not worth the money! Is it even a real film? Overall it looks cheap.	I like this movie. This is a great movie! Such a beautiful work. Surely recommend it!

Table 4: Set of insertions for the addition type according to the new label $\widehat{y}$. The words are comma-separated for "short", and each line is one piece of text for "long".

For the replacement type, each word in the input is checked against the list of replacement word sets in Tab. 5, and if the word belongs to the one set, it is changed according to the new label $\widehat{y}$. On average, 27% of input words are replaced.

Replacement word sets	$\widehat{y} = 0$	$\widehat{y} = 1$
a, an, the	a	the
in, on, at	in	on
I, you	I	you
he, she	he	she
can, will, may	can	may
could, would, might	could	might
(all forms of *be*)	is	are
(all punctuation marks)	(period)	(comma)

Table 5: Replacement word sets and their target words.

We call these modifications symmetric since inputs corresponding to both $\widehat{y} = 0$ and $\widehat{y} = 1$ are modified. We also define the asymmetric modification, where only inputs with $\widehat{y} = 1$ are modified, and those with $\widehat{y} = 0$ are left unchanged.

Metrics We use the two metrics proposed by Bastings et al. (2021): precision and normalized rank. First, we define the ground truth correlated words. For the two addition types, they are the inserted words. In the asymmetric case, instances with $\widehat{y} = 0$ does not have any words added, so we exclude them in metric value computation[1]. For the replacement type, they are the words that are in to the replacement set (but not necessarily replaced).

Let W be the set of ground truth correlated words. Using ranked importance $r(\cdot)$ in Def. 4.1, precision and normalized rank are defined as

$$\mathrm{Pr} = \frac{|\{w \in W : r(w) > L - |W|\}|}{|W|}, \qquad (12)$$

$$\mathrm{NR} = \frac{L - \min\{r(w) : w \in W\} + 1}{L}. \qquad (13)$$

Precision is the fraction of ground truth words among the the top-$|W|$ ranked words, and normalized rank is the lowest rank among ground truth words, normalized by the length L of the input. Both values are in $[0, 1]$, and higher precision and lower normalized rank values are better.

Results Tab. 6 presents the average values across the test set. Many explainers including E* score perfectly on short additions, but all struggle on other types. Nonetheless, E* still ranks comparably or favorably to other methods. Its largest advantage happens on the asymmetric long addition, because this setup matches with the computation of κ and σ: E* searches for the most important words to remove/add to maximally change/preserve the original prediction, and those words are exactly the ground truth inserted ones. For replacement and symmetric addition, the search procedure does not "reconstruct" inputs of the other class, and hence optimizing Δ fails to uncover the ground truth. This finding also suggests a mismatch between metric computation and certain ground truth types.

Conversely, vanilla gradient performs decently on ground truth types other than short addition, yet ranks at the bottom on most quality metrics (Tab. 1 and 3), again likely due to the mismatch.

	Short Addition				Long Addition				Replacement			
	Sym		Asym		Sym		Asym		Sym		Asym	
Explainer	Pr↑	NR↓	Pr↑	NR↓	Pr↑	NR↓	Pr↑	NR↓	Pr↑	NR↓	Pr↑	NR↓
Grad	0.91	0.06	0.51	0.08	0.70	0.37	0.77	0.30	0.50	0.75	0.51	0.74
IntG	0.82	0.10	0.60	0.21	0.60	0.76	0.70	0.55	0.49	0.74	0.48	0.74
LIME	1.00	0.06	1.00	0.06	0.72	0.60	0.84	0.32	0.63	0.65	0.54	0.71
SHAP	0.98	0.07	1.00	0.06	0.61	0.83	0.75	0.98	0.65	0.67	0.62	0.68
Occl	1.00	0.06	1.00	0.06	0.72	0.59	0.79	0.42	0.40	0.80	0.40	0.85
E*	1.00	0.06	1.00	0.06	0.67	0.64	0.92	0.38	0.60	0.66	0.54	0.73
Random	0.06	0.54	0.07	0.53	0.25	0.89	0.24	0.88	0.27	0.85	0.28	0.85

Table 6: Average values of precision and normalized rank of the ground truth correlated words for each explainer.

[1] This highlights an intrinsic limitation of feature attribution explanations: they cannot explain that the model predicts a class because certain features are *not* present, also observed for image classifiers (Zhou et al., 2022a).

6 Discussion

We now turn to the root cause of the solvability, its (un)desirability and circumvention.

Evaluations with Privileged Information Compared to the evaluation of explanation, that of prediction (e.g. test set accuracy) is much more straightforward without the solvability loophole. The difference, as we point out, is the use of "privileged information" in the latter. Fig. 5 shows the workflow of evaluating prediction and explanation, making every dependency explicit. When evaluating model prediction, the evaluator runs the model on the input, receives the prediction, and compares it with the ground truth label, which is emphatically *not* available to the model under evaluation. By contrast, no such privileged information is used for evaluating model explanation, allowing the explainer to solve for the interpretability metric.

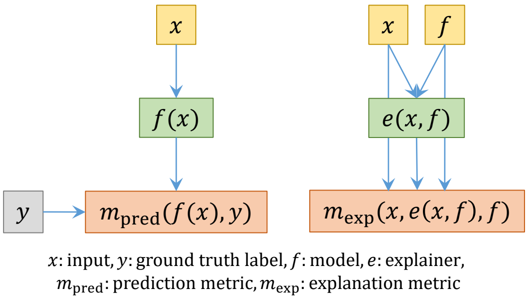

x
$f(x)$
y
$m_{\text{pred}}(f(x), y)$
x
f
$e(x, f)$
$m_{\text{exp}}(x, e(x, f), f)$
x: input, y: ground truth label, f: model, e: explainer,
m_{pred}: prediction metric, m_{exp}: explanation metric

Figure 5: The complete evaluation diagrams for model predictions (left) and explanations (right). Green boxes are the model and explainer under evaluation, which have access to the information in yellow, and orange boxes are the evaluators. Notably, prediction evaluation (e.g. accuracy) uses the ground truth label y not accessible to the model, but no such privileged information is used by the interpretability evaluation.

One way to avoid solvability is to introduce certain privileged information. In fact, this is exactly what the ground truth evaluation of Sec. 5.5 does: the ground truth correlated words are analogous to the ground truth labels in evaluating predictions, and are not available to the explainer, but it requires dataset modification and model retraining, and cannot evaluate models trained on datasets in the wild. Above all, however, the "real goal" of explanation should not be high metric values in the first place, but instead concrete instances of demonstrable utility, as discussed below.

Demonstrable Utility Fundamentally, local explanations are means to an end – the end of a better understanding of the model (Zhou et al., 2022b; Zheng et al., 2022). Thus, we argue that a definitive evaluation should exhibit its *demonstrable utility*: the presence of explanation compared to its absence, or the newly proposed explanation compared to existing ones, should lead to a measurable difference in some practically beneficial aspect.

During model development, a major concern is that the model may pick up spurious correlations, and explanations are hoped to identify them, but such capability has been called into question recently (Zhou et al., 2022a; Adebayo et al., 2022).

Before model deployment, understanding the safety and reliability of models is crucial, especially for when models take physical actions in the world such as medication prescription. Jia et al. (2021) found that model explanations are promising but currently insufficient to achieve it.

For deployed models, Bansal et al. (2021) found that existing explanation methods rarely help a human decision maker assisted by a non-perfect model (e.g. in computer-aided diagnosis), but instead exacerbate the overtrust issue. Evidence for improved human performance is another demonstration of the concrete utilities of explanations.

Demonstrating that explanations help in such scenarios would bypass discussions of solvability and directly assert their usefulness. The three listed here are by no means comprehensive, and a systematic taxonomy is valuable. Furthermore, it is likely that no single explainer is a one-size-fit-all solution. More refined knowledge of the strengths and weaknesses of each method in supporting different aspects of model understanding is highly desirable.

7 Conclusion

We demonstrate that the many interpretability evaluation metrics are *solvable*, in that there is an explicit search procedure to find the explanation that achieves the optimal metric value. Given that these metrics are used to represent explanation quality, it is not clear why heuristic explainers such as LIME and SHAP are needed.

In this paper, we use a beam search to find the explanation E^* that optimizes for comprehensiveness and sufficiency (DeYoung et al., 2020), and find E^* performing comparably or favorably in all evaluations. Thus, we advocate for more investigations into this search-based paradigm and recommend future proposals of heuristic explainers to clearly establish the ways in which they are better than E^*. We additionally discuss how to resolve the solvability issue and make evaluations more convincing and grounded in real-world setups.

Limitations

The focus of our paper is to investigate the search-based explanation that explicitly optimizes a target quality metric. While the results suggest that it is comparable or favorable to existing heuristic explainers on various technical aspects, its societal properties have not been studied. For example, Ghorbani et al. (2019) showed that many heuristic explanations can be easily manipulated and Slack et al. (2020) demonstrated that discriminative models can be carefully modified such that their discrimination is hidden by heuristic explanations. It is possible that same issues exist for the search-based explanation, and thus we advise to carefully study them before deployment.

References

Julius Adebayo, Justin Gilmer, Michael Muelly, Ian Goodfellow, Moritz Hardt, and Been Kim. 2018. Sanity checks for saliency maps. *Advances in Neural Information Processing Systems*, 31.

Julius Adebayo, Michael Muelly, Harold Abelson, and Been Kim. 2022. Post hoc explanations may be ineffective for detecting unknown spurious correlation. In *International Conference on Learning Representations*.

Julius Adebayo, Michael Muelly, Ilaria Liccardi, and Been Kim. 2020. Debugging tests for model explanations. *Advances in Neural Information Processing Systems*, 33:700–712.

David Alvarez-Melis and Tommi S Jaakkola. 2018. Towards robust interpretability with self-explaining neural networks. *Advances in Neural Information Processing Systems*, 31.

Vijay Arya, Rachel KE Bellamy, Pin-Yu Chen, Amit Dhurandhar, Michael Hind, Samuel C Hoffman, Stephanie Houde, Q Vera Liao, Ronny Luss, Aleksandra Mojsilović, et al. 2019. One explanation does not fit all: A toolkit and taxonomy of ai explainability techniques. *arXiv preprint arXiv:1909.03012*.

Gagan Bansal, Tongshuang Wu, Joyce Zhou, Raymond Fok, Besmira Nushi, Ece Kamar, Marco Tulio Ribeiro, and Daniel Weld. 2021. Does the whole exceed its parts? The effect of AI explanations on complementary team performance. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16.

Jasmijn Bastings, Sebastian Ebert, Polina Zablotskaia, Anders Sandholm, and Katja Filippova. 2021. “Will you find these shortcuts?” A protocol for evaluating the faithfulness of input salience methods for text classification. *arXiv preprint arXiv:2111.07367*.

Chun Sik Chan, Huanqi Kong, and Liang Guanqing. 2022. A comparative study of faithfulness metrics for model interpretability methods. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 5029–5038, Dublin, Ireland. Association for Computational Linguistics.

George Chrysostomou and Nikolaos Aletras. 2021. Improving the faithfulness of attention-based explanations with task-specific information for text classification. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 477–488, Online. Association for Computational Linguistics.

Jay DeYoung, Sarthak Jain, Nazneen Fatema Rajani, Eric Lehman, Caiming Xiong, Richard Socher, and Byron C. Wallace. 2020. ERASER: A benchmark to evaluate rationalized NLP models. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pages 4443–4458, Online. Association for Computational Linguistics.

Shi Feng, Eric Wallace, Alvin Grissom II, Mohit Iyyer, Pedro Rodriguez, and Jordan Boyd-Graber. 2018. Pathologies of neural models make interpretations difficult. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, pages 3719–3728, Brussels, Belgium. Association for Computational Linguistics.

Robert Geirhos, Jörn-Henrik Jacobsen, Claudio Michaelis, Richard Zemel, Wieland Brendel, Matthias Bethge, and Felix A Wichmann. 2020. Shortcut learning in deep neural networks. *Nature Machine Intelligence*, 2(11):665–673.

Amirata Ghorbani, Abubakar Abid, and James Zou. 2019. Interpretation of neural networks is fragile. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 3681–3688.

Yan Jia, John McDermid, Tom Lawton, and Ibrahim Habli. 2021. The role of explainability in assuring safety of machine learning in healthcare. *arXiv preprint arXiv:2109.00520*.

Scott Kirkpatrick, C Daniel Gelatt Jr, and Mario P Vecchi. 1983. Optimization by simulated annealing. *Science*, 220(4598):671–680.

Jiwei Li, Xinlei Chen, Eduard Hovy, and Dan Jurafsky. 2016a. Visualizing and understanding neural models in NLP. In *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pages 681–691, San Diego, California. Association for Computational Linguistics.

Jiwei Li, Will Monroe, and Dan Jurafsky. 2016b. Understanding neural networks through representation erasure. *arXiv preprint arXiv:1612.08220*.

Scott M Lundberg and Su-In Lee. 2017. A unified approach to interpreting model predictions. *Advances in Neural Information Processing Systems*, 30.

Ronny Luss, Pin-Yu Chen, Amit Dhurandhar, Prasanna Sattigeri, Yunfeng Zhang, Karthikeyan Shanmugam, and Chun-Chen Tu. 2021. Leveraging latent features for local explanations. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, pages 1139–1149.

Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. 2018. Towards deep learning models resistant to adversarial attacks. In *International Conference on Learning Representations*.

Weili Nie, Yang Zhang, and Ankit Patel. 2018. A theoretical explanation for perplexing behaviors of backpropagation-based visualizations. In *International Conference on Machine Learning*, pages 3809–3818. PMLR.

Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. "Why should I trust you?" Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1135–1144.

Alvin E Roth. 1988. *The Shapley value: essays in honor of Lloyd S. Shapley*. Cambridge University Press.

Wojciech Samek, Alexander Binder, Grégoire Montavon, Sebastian Lapuschkin, and Klaus-Robert Müller. 2016. Evaluating the visualization of what a deep neural network has learned. *IEEE Transactions on Neural Networks and Learning Systems*, 28(11):2660–2673.

Sofia Serrano and Noah A. Smith. 2019. Is attention interpretable? In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 2931–2951, Florence, Italy. Association for Computational Linguistics.

Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. 2014. Deep inside convolutional networks: Visualising image classification models and saliency maps. In *Workshop at International Conference on Learning Representations*.

Dylan Slack, Sophie Hilgard, Emily Jia, Sameer Singh, and Himabindu Lakkaraju. 2020. Fooling lime and shap: Adversarial attacks on post hoc explanation methods. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pages 180–186.

Richard Socher, Alex Perelygin, Jean Wu, Jason Chuang, Christopher D. Manning, Andrew Ng, and Christopher Potts. 2013. Recursive deep models for semantic compositionality over a sentiment treebank. In *Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing*, pages 1631–1642, Seattle, Washington, USA. Association for Computational Linguistics.

Mukund Sundararajan, Ankur Taly, and Qiqi Yan. 2017. Axiomatic attribution for deep networks. In *International Conference on Machine Learning*, pages 3319–3328. PMLR.

Julia K Winkler, Christine Fink, Ferdinand Toberer, Alexander Enk, Teresa Deinlein, Rainer Hofmann-Wellenhof, Luc Thomas, Aimilios Lallas, Andreas Blum, Wilhelm Stolz, et al. 2019. Association between surgical skin markings in dermoscopic images and diagnostic performance of a deep learning convolutional neural network for melanoma recognition. *JAMA dermatology*, 155(10):1135–1141.

Yiming Zheng, Serena Booth, Julie Shah, and Yilun Zhou. 2022. The irrationality of neural rationale models. In *Proceedings of the 2nd Workshop on Trustworthy Natural Language Processing (TrustNLP)*.

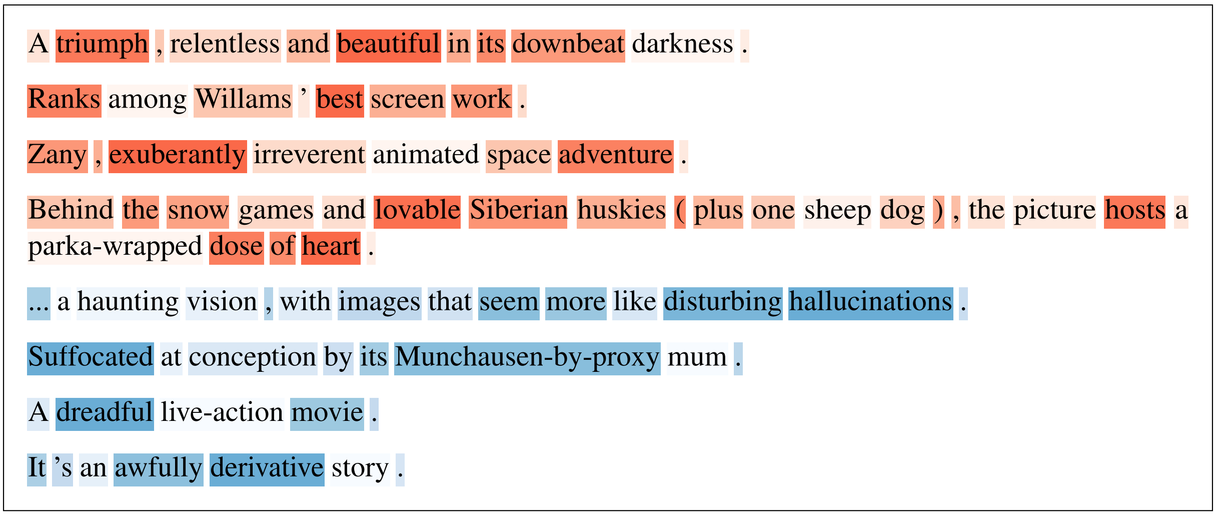
Yilun Zhou, Serena Booth, Marco Tulio Ribeiro, and Julie Shah. 2022a. Do feature attribution methods correctly attribute features? In *AAAI Conference on Artificial Intelligence*.

Yilun Zhou, Adithya Renduchintala, Xian Li, Sida Wang, Yashar Mehdad, and Asish Ghoshal. 2021. Towards understanding the behaviors of optimal deep active learning algorithms. In *International Conference on Artificial Intelligence and Statistics*, pages 1486–1494. PMLR.

Yilun Zhou, Marco Tulio Ribeiro, and Julie Shah. 2022b. ExSum: From local explanations to model understanding. In *Annual Conference of the North American Chapter of the Association for Computational Linguistics*. Association for Computational Linguistics.

A Additional Qualitative Examples of the E* Explanation

Fig. 6 presents more visualizations of E* explanations. These examples suggest that E* mostly focus on words that convey strong sentiments, which is a plausible working mechanism of a sentiment classifier.



A triumph , relentless and beautiful in its downbeat darkness .

Ranks among Willams ' best screen work .

Zany , exuberantly irreverent animated space adventure .

Behind the snow games and lovable Siberian huskies (plus one sheep dog) , the picture hosts a parka-wrapped dose of heart .

... a haunting vision , with images that seem more like disturbing hallucinations .

Suffocated at conception by its Munchausen-by-proxy mum .

A dreadful live-action movie .

It 's an awfully derivative story .

Figure 6: More E* explanations. The shade of background color represents feature importance.

B An Analysis on the Rank$_{\text{Ins}}$ Metric

As introduced in App. 2, this metric evaluates the monotonicity of the model prediction curve when more important features are successively inserted into an empty input. While this expectation seems reasonable, it suffers from a critical issue due to the convention in ranking features: if a feature contributes *against* the prediction, such as a word of sentiment opposite to the prediction (e.g. a positive prediction on "Other than the story plot being a bit boring, everything else is actually masterfully designed and executed."), it should have negative attribution and the convention is to put them lower in the rank (i.e. less important) than those have zero contributions. This implementation leads to the correct interpretation of all other metric values.

However, under this convention, the first few words added to the empty input should decrease the model prediction and then increase it, leading to a U-shaped curve. In fact, it is the comprehensiveness curve shown in Fig. 3, flipped both horizontally (because features are inserted rather than removed) and vertically (because the plotted quantity is the model prediction rather than change in prediction). Thus, a deeper U-shape should be preferred, but it is less monotonic. This also explains why the random attribution baseline achieves such a high ranking correlation: as we randomly add features from the empty string to the full input, on average the curve should be a more or less monotonic interpolation between model predictions on empty and full inputs, which has better monotonicity rank correlation than the U-shape.

It is not clear how to fix the metric. Previous works that proposed (Luss et al., 2021) or used (Chan et al., 2022) this metric often ignored the issue. One work (Arya et al., 2019) filtered out all features of negative attribution values and evaluate the rank correlation only on the rest. This, however, is easily manipulatable by an adversary. Specifically, an explainer could shift all attribution values down such that only the most positive one has a non-negative value. This change results in a perfect correlation as long as removing most positive feature induces a decrease in model prediction – an especially low requirement to satisfy. Empirically, we found that inserting features based on their (unsigned) magnitude barely affects the result either. Thus, we argue that this metric is not a good measurement of explanation quality.

C Visualization of Perturbation Effects

Fig. 7 visually presents the random perturbation, with different standard deviation s of the Gaussian noise. In each panel, the top row orders the features by their ranked importance, from least important on the left to most on the right, and the bottom row orders the features with perturbed ranked importance, with lines connecting to their original position. For example, in the top panel for $s = 1$, the perturbation swaps the relative order of the two least important features on the left.

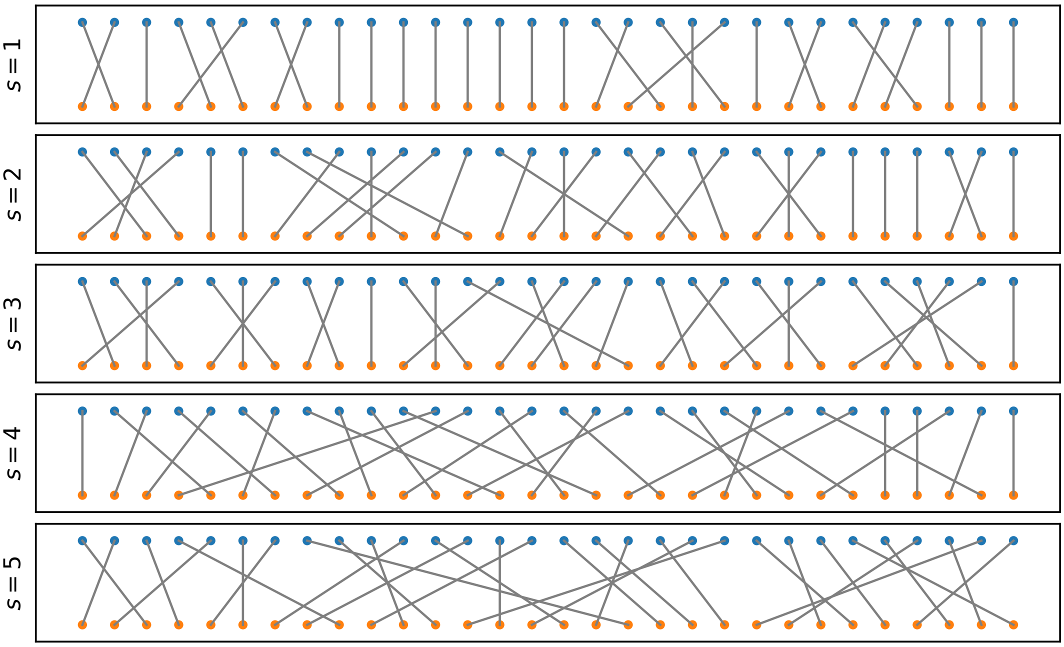


Figure 7: Visualization of rank perturbation under different values of s.

D Another Assessment on the Explainer-Attacking-Model Behavior

We describe another experiment to assess whether the explanations exploit the adversarial vulnerability of the model. While it is possible that the model could use some shortcuts (Geirhos et al., 2020), we would expect it to predominantly use sentiment-conveying words, as it achieves high accuracy and no such shortcuts are known for the dataset. In this case, we should expect an explainer that do not adversarially exploit the model to give attributions for words correlated with their sentiment values, while an explainer that attacks the model would rate words that are "adversarial bugs" to be more important.

Conveniently, the SST dataset provides human annotations of the polarity score between 0 and 1 for each word, where 0 means very negative, 1 means very positive, and 0.5 means neutral. We compute the alignment between the attribution values (for the positive class) and this score for each word. Given a sentence $x = (x_1, ..., x_L)$ with explanation $e = (e_1, ..., e_L)$ and word polarity score $s = (s_1, ..., s_L)$, the alignment is defined as the Spearman rank correlation coefficient $\rho(e, s)$. Since the vanilla gradient only produces non-negative values, it is impossible to identify whether a word contributes *to* or *against* the positive class, and we exclude it from the analysis.

Fig. 8 plots the distribution of rank correlations among the test set instances, with the average shown as the bar and also annotated on the horizontal axis. Although no method achieves very high alignment, E* is the second-highest, after LIME. Thus, giving out assumption that high-polarity words are the indeed genuine signals used by the model for making predictions, we can conclude that E* does not adversarially exploit the model for its vulnerability more severely than the heuristic explainers.

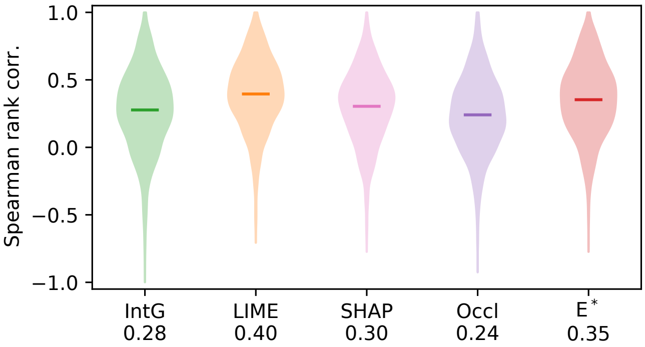


Figure 8: Spearman rank correlation coefficient between intrinsic word polarity score and attribution value.