Robustness and Usefulness in AI Explanation Methods

Erick Galinkin*

March 9, 2022

Abstract

Explainability in machine learning has become incredibly important as machine learning-powered systems become ubiquitous and both regulation and public sentiment begin to demand an understanding of how these systems make decisions. As a result, a number of explanation methods have begun to receive widespread adoption. This work summarizes, compares, and contrasts three popular explanation methods: LIME, SmoothGrad, and SHAP. We evaluate these methods with respect to: robustness, in the sense of sample complexity and stability; understandability, in the sense that provided explanations are consistent with user expectations; and usability, in the sense that the explanations allow for the model to be modified based on the output. This work concludes that current explanation methods are insufficient; that putting faith in and adopting these methods may actually be worse than simply not using them.

1 Introduction

Machine learning has become a ubiquitous part of life for us. These algorithms aim to predict, either via classification or regression, information about a particular input. The trouble comes in that, as Doshi-Velez and Kim [11] put it, any single metric is necessarily an incomplete description of the real world. Given the influence these systems have in our lives, people seek to understand precisely why a model made a particular decision. To this end, research efforts around interpreting and explaining the predictions of models have sprung up and have fallen into two overarching families: intrinsically interpretable models and post-hoc explanation methods. The results of the methods are typically quite similar, but while interpretable models aim to be sufficiently simple that their predictions are easily reasoned about, post-hoc explanation methods take a trained model that may be extremely complex and construct explanations from properties of the model. This work focuses primarily on popular explanation methods applied to trained models rather than inherent interpretability.

*erick_galinkin@rapid7.com
Explanation methods are of particular concern because of the way that they influence human behavior. Despite the challenges in defining terms like interpretability in concrete terms [21], explanations are important for improving trust and can also improve the speed at which human auditors perform their work [30]. For some users, the mere presence of an explanation increases that user’s trust in a model, even when the explanations are incorrect [6]. In other cases, even data scientists who build models tend to rely too heavily on these interpretability tools [19], demonstrating a failure to use the tool’s appropriately. These challenges, and others, are detailed in Section 4.

2 Background

This work reflects on a number of explanation methods – namely LIME, SmoothGrad, and SHAP. These methods have begun to see adoption in industry [13] and are popular for their ease of implementation. To facilitate the discussion in Section 3 we introduce the motivation and implementation of these methods below.

2.1 Local Interpretable Model-Agnostic Explanations (LIME)

Local Interpretable Model-Agnostic Explanations (LIME) [29] is an explanation method that aims to explain the predictions of any classifier, irrespective of complexity or linearity. This is accomplished through an interpretable representation that locally approximates the overall classifier. The interpretable representation is derived from a class of potentially interpretable models – limited in part by the complexity of the model, denoted $\Omega(g)$. In this case, examples of complexity include tree depth or the number of non-zero weights of a linear model.

In addition to minimizing complexity, LIME also seeks a model that minimizes the locality-aware loss, or so-called fidelity function $L$ for an input $x$. $L$ is a function that measures how good an interpretable model $g$ is at approximating a classifier $f$ in a neighborhood $\pi_x$ of $x$. Formally, given an input $x$, a classifier $f$, and a class of potentially interpretable models $G$, the explanation produced by LIME is obtained by:

$$\xi(x) = \arg\min_{g \in G} L(f, g, \pi_x) + \Omega(g)$$  \hspace{1cm} (1)

LIME then perturbs and samples the space around each instance of interest, $x$, constructing representations and labels for those representations. The new samples are weighted by their distance from $x$. These representations and labels are then used to select and train the model satisfying Equation 1. This means that the explanation model used for a particular instance $x$ is the model $g$ that is closest to the classifier $f$ with minimal model complexity $\Omega(g)$. In practice, $\Omega(g)$ is a hyperparameter [25]. For example, if we want to use linear regression models as our locally interpretable model, we select the number of parameters $K$ to be used in the model.
2.2 SmoothGrad

SmoothGrad [36] is a gradient-based explanation method that builds on work like Saliency Maps [34] and GradCAM [31]. Crucially, SmoothGrad is not, on its own, an explanation method, but rather an extension of any existing gradient-based explanation method. When we refer to SmoothGrad on its own, we refer to implementations like iNNvestigate [3] where it complements so-called “vanilla” gradient methods.

These gradient-based methods take advantage of the backpropagation algorithm used in training neural networks, particularly convolutional neural networks used in image classification. SmoothGrad was developed in response to two issues in gradient-based explanation methods:

1. The issue of one feature with a strong global effect but a small local derivative “saturating” the sensitivity map
2. Noisy gradients as a result of the class sensitivity function’s derivative fluctuating locally

SmoothGrad aims to solve these problems by generating multiple versions of an image of interest $x$ by adding noise to it. Pixel attribution maps – heatmaps like those generated in Selvaraju et al. [31] – are then created for all of these images, and those maps are then averaged together. The idea here is that adding some noise sampled from a Gaussian distribution averaged over multiple maps can smooth the local gradient fluctuations and lead to better maps.

2.3 Shapley Additive Explanations (SHAP)

Shapley Additive Explanations (SHAP) [23] is an explainability method that leverages a game theoretic approach to understand model predictions. The work was motivated as an attempt to unify six different methods for interpreting model predictions, including LIME. SHAP works by assigning an importance value to each feature for each prediction using Shapley value estimation methods. The Shapley value [32] is a construct from cooperative game theory named for Lloyd Shapley that seeks to distribute the total gain in utility across a coalition of players according to each player’s marginal contribution. Formally, given a characteristic function $v : 2^n \rightarrow \mathbb{R}, v(\emptyset) = 0$ that maps a set of players to a value for that coalition, the set of all players $N$ and a coalition of players $S \subseteq N$, a fair distribution for each player $i$ in a coalition $S$ is given by:

$$\phi_i(v) = \sum_{|S \subseteq N \setminus \{i\}|} \frac{|S|!(|N| - |S| - 1)!}{|N|!} (v(S \cup \{i\}) - v(S)) \quad (2)$$

Theorem 1 of Lundberg and Lee [23] shows that only one possible explanation model for the properties of local accuracy, missingness, and consistency holds for additive feature
attribution methods – explanation models that are linear functions of binary variables – the Shapley value. Despite the fact that exactly computing Shapley values is NP-Hard, the paper develops model-agnostic approximations by assuming feature independence and model linearity. The paper describes two classes of approximations: model-agnostic approximations and model-specific approximations. The model-agnostic approximation introduced in this initial work is called Kernel SHAP, which leverages linear LIME with Shapley values. The model-specific approximations in the initial paper handle linear models and deep neural networks using techniques from DeepLIFT [33].

The initial model was extended to provide visual explanations in later work [24]. A further extension of SHAP [22] tackled the problems associated with model-specific approximations of nonlinear, tree-based models. Tree SHAP, as the author calls it, leverages feature perturbations to locally estimate the interaction index, a game theoretic concept that follows from generalization of the Shapley value properties.

3 Comparison of Explainability Methods

The three explainability methods above are all post-hoc methods that give a view into machine learning black boxes. As discussed in Section 1, there is growing interest in leveraging explainability and interpretability methods in practice. This means that is is prudent to understand the strengths and shortcomings of each method, and leverage the right one for our task. Table 1 summarizes some of the commonalities and differences between the methods, which we detail in this section.

| Methodology | Local Explanation | Visualizable | Model Agnostic |
|-------------|-------------------|--------------|----------------|
| LIME        | Perturbation      | ✓            | X              | ✓              |
| SmoothGrad  | Gradient          | ✓            | ✓              | X              |
| SHAP        | Perturbation      | ✓            | ✓              | ✓              |

Table 1: Summary of LIME, SmoothGrad, and SHAP

3.1 Methodology

The three methods we consider fall under two different methodologies – perturbation and gradient. Perturbation methods add some noise to inputs and sample the space of perturbed inputs to assess the effect of small changes in the space. Gradient-based methods instead use the gradients computed for given inputs to explain model predictions.

Agarwal et al. [1] consider a variant of LIME for continuous data called C-LIME and compare it directly to SmoothGrad. Interestingly, though ado much has been made of the differences between perturbation and gradient-based explanations, Agarwal et al. demonstrate that given the same Gaussian distribution for perturbations and gradient computation, C-LIME and SmoothGrad yield the same explanation in expectation. This suggests
that the methodology of the explanation is, on average, not meaningful to distinguish methods.

3.2 Local Explanation

We define local explainability as the ability to interrogate and explain particular examples from the data. All three of the methods we consider here offer local explanations for single predictions. This is a property that is often desirable for legal and regulatory reasons, since it is often individual predictions that lead to negative outcomes for individuals.

3.3 Visualizable

Visualizations are valuable tools for communicating data concisely in ways that humans quickly and easily understand [40]. Consequently, having explanations methods that lend themselves to visualizations can improve understanding and interpretation. SmoothGrad can be used with any number of gradient-based methods, but its use with the so-called “vanilla” gradient as mentioned in Section 2.2 lends itself to the creation of heat maps.

SHAP, though it does not produce heat maps on images, has a Python package ¹ that generates force plots which show how each feature contributes to the model output. This method is used for individual predictions but can also be used across entire datasets to understand how the model treats the entirety of the dataset. In cases where we want to understand the influence of a single feature, SHAP offers a way to visualize the impact of that single feature across the dataset.

LIME, on the other hand, does not lend itself to a natural visualization. The relatively simple nature of the LIME model means that variable importance measures or partial dependence plots can be used to visualize attributes of the more interpretable model, but these visualizations are less direct than those produced by SmoothGrad or SHAP. Specifically, the visualization would be informative about the surrogate model around the point of interest, and would not give a view into how the larger model made the prediction relative to the input in question.

3.4 Model Agnostic

Model agnostic methods are able to be used across a variety of model types. By the No Free Lunch Theorem [41], we know that there is no single model that is optimal for all tasks. This means that in practice, different models will be used for different tasks and those models may require explanation in different ways. Moreover, the way that data is input to the model can vary wildly – images and video data structures often look quite different from text, and all of these require different handling and processing methods from tabular data. Model agnostic explanation methods aim to handle any of these input methods.

¹https://github.com/slundberg/shap
LIME specifically aims to be model-agnostic and achieves this by uncovering locally-interpretable models. SHAP, building on the foundation of LIME, also inherits this property. Though some specifics between e.g. KernelSHAP [23] and TreeExplainer [22] differ, the core of the methods remain the same. This means that the skills associated with interpreting e.g. Shapley values are transferrable across models.

SmoothGrad is not model agnostic and is only usable within differentiable models. In fact, SmoothGrad is specifically useful in the case of convolutional neural networks used for computer vision applications. This makes it a powerful tool for identifying where in an image the model is “paying attention”, but limits the usefulness of the method in general.

4 Weaknesses of Explainability Methods

Model trust is a critically important concept, gaining the attention of many, including the National Institute of Standards and Technology [38] and the parliament of the European Union [8]. This concept of trust, however, builds on a shaky foundation. In particular, nearly all legislation proposed to date includes a requirement for model interpretability. Lipton [21] offers a stunning rebuke of the term itself, as the term has no agreed upon meaning. In essence, the question becomes not whether a model is interpretable or not, but rather to whom and under what circumstances model predictions can be understood.

4.1 Human Factors in Explanations

One critique leveled at fairness in machine learning [12] is the notion that one must conceive of an “ideal world” against which the current world is compared. This can lead to unexpected negative outcomes for certain groups and notions of fairness that leave everyone worse off: for example, a perfectly fair judge who always denies bail and parole. The weaknesses of metrizable fairness then promotes the desire for explanations – why was bail denied?

A bevy of work has shown that although explainability methods have been widely promoted, the explanations provided by the likes of LIME, SmoothGrad, and SHAP can also range from being useless to outright harmful. Kaur et al. [19] show that data scientists tend to misuse and over-rely on explanations from tools like SHAP. Moreover, decision-makers often defer to algorithmic decision support systems [15] and struggle to use the algorithms effectively – often underperforming compared to both humans who are not assisted and the algorithms themselves [20]. Model-agnostic methods are not alone here, as Grad-CAM [31] has been shown to perform quite poorly on tasks it was specifically designed to excel at [27] under benchmark conditions that are not sufficiently realistic.

Explainability often uses healthcare for piloting its methods, likely due to the superhuman performance of machine learning methods on a variety of medical tasks [7, 18, 26]. SHAP in particular has been used in healthcare contexts [21] and has been touted as a machine learning explainability method with promise to improve healthcare worker trust.
in algorithms. This is very likely to be true, as even when users are presented explanations 
are wrong [6] or completely random [37], they tend to believe that the algorithm is correct. Indeed, in the healthcare imaging context [14], localizing a region of an image does not inform a human exactly what in that region the model considered useful. Combining these two phenomena – a lack of clarity in the explanation paired with human deference to decision support algorithms – is ultimately putting a human in the loop purely for decoration in the best case.

4.2 Robustness of Explainers

Beyond the human factors, the theoretical properties of explanation methods leaves much 
to be desired. Agarwal et al. [1] investigate robustness for C-LIME and SmoothGrad in cer-
tain settings, but find that the robustness is sensitive to variance in the data. Robustness is 
a particularly valuable attribute for explanations, as humans expect the important factors for data that are “near” each other to be similar. Despite the equivalence of perturbation and gradient-based methods in expectation, perturbation-based methods are empirically worse [4] at providing consistent explanations given small modifications to the input. Moreover, since there are so many models and explanation methods that achieve comparable performance, this phenomenon may lead to selecting models on the basis of how pleasing the explanations are [16] without regard for the consistency of those explanations. Rahnama and Boström [28] also find that LIME is not robust to changes in the distribution of the data – a common occurrence in production applications of machine learning.

This lack of robustness also allows for explainers to be “tricked” [35] by models that aim to offer pleasing explanations, even when those explanations do not provide visibility into the model itself. In image classification, similarly, so-called “adversarial examples” [39] – inputs with specially-crafted perturbations that are imperceptible to humans – can be crafted to arbitrarily change saliency maps [10,17]. As a result of this, a model designer who is for whatever reason disinterested in removing bias from their model is able to provide explanations with whatever properties they wish – a property that Aivodji et al. [2] have termed “fairwashing”.

Model explanations are, of course, also impacted by human behavior that is used as input. In recent work, Arora et al. [5] ask participants to edit hotel reviews in such a way that a human reader can still derive whether a review is still positive, negative, or mixed, while model confidence for the predicted class is minimized. The study finds that for BERT [9], a transformer model widely used in natural language processing, local explanations via LIME and Integrated Gradients offer no additional ability for participants to reduce the confidence of the model, while a linear model trained only on the predictions of the BERT model offered participants significantly more ability to change the label associated with the sample. Ultimately, this demonstrates that the relative utility of the local explanations is lower than simply using feature coefficients from a linear model that approximates the global model.
5 Conclusion

Post-hoc explanation methods offer significant opportunity to improve the usability and human comprehensibility of machine learning methods. However, current popular methods face a variety of problems from both a theoretical and sociotechnical perspective. Though these problems may not be unsolvable or inherent, further investigation is needed on how to increase the robustness and usefulness of explanations. Given the concomitant phenomena of human deference to decision support systems, human willingness to accept incorrect explanations, a lack of robustness for explanations, and a lack of theoretical guarantees for extant explanation methods, the idea of a “human-in-the-loop” serves as nothing more than a security blanket. In order to deal with model interpretability and explainability, more foundational work needs to be done to formalize problems in interpretability and consider ideas around causality and contestability. Counterfactual explanations offer a potential path forward, though extant counterfactual generation methods have their own weaknesses and biases.

References

[1] Agarwal, S., Jabbari, S., Agarwal, C., Upadhyay, S., Wu, S., and Lakkaraju, H. Towards the unification and robustness of perturbation and gradient based explanations. In International Conference on Machine Learning (2021), PMLR, pp. 110–119.

[2] Aïvodji, U., Arai, H., Fortineau, O., Gambs, S., Hara, S., and Tapp, A. Fairwashing: the risk of rationalization. In International Conference on Machine Learning (2019), PMLR, pp. 161–170.

[3] Alber, M., Lapuschkin, S., Seegerer, P., Hägele, M., Schütt, K. T., Montavon, G., Samek, W., Müller, K.-R., Dähne, S., and Kindermans, P.-J. Investigate neural networks! Journal of Machine Learning Research 20, 93 (2019), 1–8.

[4] Alvarez-Melis, D., and Jaakkola, T. S. On the robustness of interpretability methods. ICML 2018 Workshop on Human Interpretability in Machine Learning (2018).

[5] Arora, S., Pruthi, D., Sadeh, N., Cohen, W. W., Lipton, Z. C., and Neubig, G. Explain, edit, and understand: Rethinking user study design for evaluating model explanations. In 36th AAAI Conference on Artificial Intelligence (2022).

[6] Bansal, G., Wu, T., Zhou, J., Fok, R., Nushi, B., Kamar, E., Ribeiro, M. T., and Weld, D. 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* (2021), pp. 1–16.

[7] Choudhury, A., Asan, O., et al. Role of artificial intelligence in patient safety outcomes: systematic literature review. *JMIR medical informatics* 8, 7 (2020), e18599.

[8] Commission, E., et al. Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. *COM (2021) 206* (2021).

[9] Devlin, J., Chang, M.-W., Lee, K., and Toutanova, K. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805* (2018).

[10] Dombrowski, A.-K., Alber, M., Anders, C., Ackermann, M., Müller, K.-R., and Kessel, P. Explanations can be manipulated and geometry is to blame. *Advances in Neural Information Processing Systems 32* (2019).

[11] Doshi-Velez, F., and Kim, B. Towards a rigorous science of interpretable machine learning. *arXiv* (2017).

[12] Fazelpour, S., and Lipton, Z. C. Algorithmic fairness from a non-ideal perspective. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (2020), pp. 57–63.

[13] Gade, K., Geyik, S. C., Kenthapadi, K., Mithal, V., and Taly, A. Explainable ai in industry. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* (2019), pp. 3203–3204.

[14] Ghassemi, M., Oakden-Rayner, L., and Beam, A. L. The false hope of current approaches to explainable artificial intelligence in health care. *The Lancet Digital Health* 3, 11 (2021), e745–e750.

[15] Green, B., and Chen, Y. The principles and limits of algorithm-in-the-loop decision making. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[16] Hancox-Li, L. Robustness in machine learning explanations: does it matter? In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (2020), pp. 640–647.

[17] Heo, J., Joo, S., and Moon, T. Fooling neural network interpretations via adversarial model manipulation. *Advances in Neural Information Processing Systems 32* (2019).
[18] Hosny, A., Parmar, C., Quackenbush, J., Schwartz, L. H., and Aerts, H. J. Artificial intelligence in radiology. *Nature Reviews Cancer* 18, 8 (2018), 500–510.

[19] Kaur, H., Nori, H., Jenkins, S., Caruana, R., Wallach, H., and Worman Vaughan, J. Interpreting interpretability: understanding data scientists’ use of interpretability tools for machine learning. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (2020), pp. 1–14.

[20] Lai, V., and Tan, C. On human predictions with explanations and predictions of machine learning models: A case study on deception detection. In *Proceedings of the conference on fairness, accountability, and transparency* (2019), pp. 29–38.

[21] Lipton, Z. C. The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. *Queue* 16, 3 (2018), 31–57.

[22] Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., Katz, R., Himmelfarb, J., Bansal, N., and Lee, S.-I. From local explanations to global understanding with explainable ai for trees. *Nature Machine Intelligence* 2, 1 (2020), 2522–5839.

[23] Lundberg, S. M., and Lee, S.-I. A unified approach to interpreting model predictions. In *Proceedings of the 31st international conference on neural information processing systems* (2017), pp. 4768–4777.

[24] Lundberg, S. M., Nair, B., Vavilala, M. S., Horibe, M., Eisses, M. J., Adams, T., Liston, D. E., Low, D. K.-W., Newman, S.-F., Kim, J., et al. Explainable machine-learning predictions for the prevention of hypoxaemia during surgery. *Nature Biomedical Engineering* 2, 10 (2018), 749.

[25] Molnar, C. *Interpretable machine learning*. Lulu. com, 2020.

[26] Oren, O., Gersh, B. J., and Bhatt, D. L. Artificial intelligence in medical imaging: switching from radiographic pathological data to clinically meaningful endpoints. *The Lancet Digital Health* 2, 9 (2020), e486–e488.

[27] Prakash, E. I., Shrikumar, A., and Kundaje, A. Towards more realistic simulated datasets for benchmarking deep learning models in regulatory genomics. In *Machine Learning in Computational Biology* (2022), PMLR, pp. 58–77.

[28] Rahnama, A. H. A., and Boström, H. A study of data and label shift in the lime framework. *2019 NeurIPS Workshop on Human-Centric Machine Learning* (2019).

[29] Ribeiro, M. T., Singh, S., and Guestrin, C. “ 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* (2016), pp. 1135–1144.
[30] Schmidt, P., and Biessmann, F. Quantifying interpretability and trust in machine learning systems. *AAAI-19 Workshop on Network Interpretability for Deep learning* (2019).

[31] Selvaraju, R. R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., and Batra, D. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proceedings of the IEEE international conference on computer vision* (2017), pp. 618–626.

[32] Shapley, L. Quota solutions op n-person games1. *Edited by Emil Artin and Marston Morse* (1953), 343.

[33] Shrikumar, A., Greenside, P., and Kundaje, A. Learning important features through propagating activation differences. In *Proceedings of the 34th International Conference on Machine Learning* (06–11 Aug 2017), D. Precup and Y. W. Teh, Eds., vol. 70 of *Proceedings of Machine Learning Research*, PMLR, pp. 3145–3153.

[34] Simonyan, K., Vedaldi, A., and Zisserman, A. Deep inside convolutional networks: Visualising image classification models and saliency maps. *arXiv preprint arXiv:1312.6034* (2013).

[35] Slack, D., Hilgard, S., Jia, E., Singh, S., and Lakkaraju, H. Fooling lime and shap: Adversarial attacks on post hoc explanation methods. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (2020), pp. 180–186.

[36] Smilkov, D., Thorat, N., Kim, B., Viegas, F., and Wattenberg, M. Smoothgrad: removing noise by adding noise. *International Conference on Machine Learning Workshop on Visualization for Deep Learning* (2017).

[37] Springer, A., Hollis, V., and Whittaker, S. Dice in the black box: User experiences with an inscrutable algorithm. In *2017 AAAI Spring Symposium Series* (2017).

[38] Stanton, B., and Jensen, T. Trust and artificial intelligence, 2021-03-02 05:03:00 2021.

[39] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., and Fergus, R. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199* (2013).

[40] Tufte, E. R., McKay, S. R., Christian, W., and Matey, J. R. Visual explanations: Images and quantities, evidence and narrative, 1998.

[41] Wolpert, D. H., and Macready, W. G. No free lunch theorems for optimization. *IEEE transactions on evolutionary computation* 1, 1 (1997), 67–82.