Testing the effectiveness of saliency-based explainability in NLP using randomized survey-based experiments

1st Adel Rahimi
Procter & Gamble
Singapore
rahimi.a@pg.com

2nd Shaurya Jain
Singapore Management University
Singapore
shauryaj.2019@economics.smu.edu.sg

Abstract—
As the applications of Natural Language Processing (NLP) in sensitive areas like Political Profiling, Review of Essays in Education, etc. proliferate, there is a great need for increasing transparency in NLP models to build trust with stakeholders and identify biases. A lot of work in Explainable AI has aimed to devise explanation methods that give humans insights into the workings and predictions of NLP models. While these methods distill predictions from complex models like Neural Networks into consumable explanations, how humans understand these explanations is still widely unexplored. Innate human tendencies and biases can handicap the understanding of these explanations in humans, and can also lead to them misjudging models and predictions as a result. We designed a randomized survey-based experiment to understand the effectiveness of saliency-based Post-hoc explainability methods in Natural Language Processing. The result of the experiment showed that humans have a tendency to accept explanations with a less critical view.

Index Terms—AI Explainability, Machine Learning, Human-centric AI, XAI

I. INTRODUCTION

Machine Learning projects in the past relied on human knowledge and were easily comprehensible by both developers and end-users. For example, decision trees have been widely used for fraud detection [1]. However, the surge in popularity of Deep Neural Network (DNN) based models in the previous decade, due to their potential to produce more accurate results, has abated this comprehensibility. An example is the Convolutional Neural Network developed by Krizhevsky that was able to achieve “top-1 and top-5 error rates of 39.7% and 18.9%” [2] on Imagenet [3] comparing that to the second place error rate that was 26.2% on the top-5 error rate. Such superior performance of DNNs has come at the cost of explainability as they can comprise up to millions or even billions of parameters [4] [5] whose synergy in arriving at the final output is often indecipherable. Moreover, these models are considered to be ‘black boxes’, where not only the end-users but also the developers are unaware of their inner workings.

This reduced explainability has compromised the trust various stakeholders have in these models, despite their accurate results [6]. Transparency breeds trust in humans, and it is important to create transparency through explainability of these complex models [7]. It is only becoming more vital as AI gains foothold in making critical – and in some cases, fatal – decisions in sensitive areas like Healthcare, Finance, Automated Driving, and such-like [8] [9] [10]. The true potential of these recent advancements in AI can only be realised if the various stakeholders manage to discern the working of AI models and how their predictions are produced, as that is necessary to incorporate trust. For example, 83% of people do not understand automated decision-making systems in the criminal justice system, and subsequently, 60% oppose its use in the domain [11]. But besides securing the buy-in of end-users and developers through building trust, AI explainability also has the potential of identifying AI inaccuracies prior to deployment. This is crucial considering that black-box machine learning models have led to unjustified social ills, like unfavourable parole denials and credit decisions based on race [12].

This has led to the creation of Explainable AI (XAI), a subfield in AI which focuses on explaining AI decisions in human-understandable ways. Explainability itself is not a new concept [13]; Explanations of AI systems have been used to debug AI systems already [14].

While model interpretability can be augmented through restricting their complexity, this can limit the effectiveness of the models [15]. As such, there has been an explosion of work around post-hoc analysis in XAI, whereby methods are devised to explain the models post-training without aiming to make the models inherently interpretable [16]. These recent developments are able to distil predictions from complex models like Neural Networks into simple explanations that can be consumed by both developers and end-users alike. However, this points the torch to the similarity between these explanations and human understanding [17]. That is, whether these explanations of AI predictions and models are understood by humans as intended is still an open question. Innate human tendencies, biases, etc. can handicap the effectiveness of these explanations in humans accurately assessing predictions and models, and can even have the reverse of the intended outcome. This gap between explanation and understanding can...
be dangerous, especially in fields like healthcare, as it can lead to stakeholders considering incorrect models to be correct, and vice-versa. These necessitate more work to be done in this field.

The need for explainable AI is particularly important in Neural Network based NLP models — a field which is gaining foothold in making pertinent decisions, and hence, requires transparency. For example, NLP are in inchoate stages of being used for political-profiling for elections surveys [18]. Hence, NLP can heavily influence actual election outcomes being used for political-profiling for elections surveys [18]. NLP-based models are also being used at a large scale in education for essay scoring. An example of this is evaluation of essays [20]. Such important applications make NLP a pertinent AI area for explainability.

II. BACKGROUND

There are many definitions delineating what “interpretation” and “explanation” mean in the context of AI. Motavan et. al have drawn a distinction between the two [21]. They describe “Interpretability” as the ability to “mapping of an abstract concept into a domain that humans can make sense of”. For instance, text, symbols, images, etc. can help humans interpret the content and concept that they represent. “Explainability”, on the other hand, has been put forth as “the collection of features of the interpretable domain that contribute to a certain decision” [21]. An example of this would be a heatmap highlighting the pixels that contributed the most to the categorization of an image. With the increasing complexity of AI models, the focus of AI ethics has shifted from making models inherently interpretable to explaining their decisions.

Inherently Explainable AI models are white-box models which are transparent by design. By delineating the most important parameters considered, they provide an intuitive understanding of why the model has predicted a certain data point as belonging to a certain class. Some common examples of Inherently Explainable AI models are Decision Trees [22] and Linear Predictors. However, more complex problems might not be solved by Inherently Explainable AI models and require black-box models e.g. Deep Learning [23] [24].

The most popular methods for explainability can be summarized into three main categories spanning the entire cycle of modeling: Pre-modeling explainability [25], Modeling explainability or explainable modeling [26], and Post-modeling explainability [27].

Pre-modeling explainability focuses on the study of the input. It is the most rudimentary explainability method, and it comprises inspection of the input through plotting the data distribution, analyzing different classes, and even showing word tokens and class labels in the case of NLP. Such data exploration does not directly explain a model but provides useful insight into the model’s behavior. For example, imbalance in the dataset can justify why the classification performance is subpar on underrepresented labels.

Modeling explainability methods rely on the model — rather than the data — to provide understanding to the end-user. These are the aforementioned Inherently Explainable AI models that are easy to understand due to the explicitness and the quantifiable number of parameters. Black-box models can not be explained through modeling-explainability methods.

A post-modeling or post-hoc XAI method produces approximations of black-box machine learning models in the form of simpler surrogate models, with a trained AI model as an input [28]. The approximations are constructed on the local behavior of a black-box model for a given input space. The main properties of such proxy models are their inherent explainability and their local faithfulness to the original model to be able to extrapolate its behavior. These simpler surrogate models can shed light on the decision logic of the black-box models through simple and understandable representations e.g. natural language, heatmaps, feature importance scores, etc. This can in turn assist human assessors in understanding and critiquing the black-box machine learning models after they are productionized. For example, the users can understand the importance of various features, highlight errors that the model is prone to, and discern biases in the model or data [29]. Some well-known examples of these methods and packages are SHapley Additive exPlanations (SHAP) [30] [31], LIME [32], DeepLIFT [33], Interpret ML [34], and AllenNLP Interpret [35].

A number post-hoc methods derive feature importance by manipulating real samples, observing the change in the output given the changed samples, and generating a simple model that mimics the original model’s behavior in the original samples’ neighborhood. An example of such a method is Local Interpretable Model-agnostic Explanations (LIME) [36]. However, the aforementioned manipulation is done at random to produce the neighboring instances, and the local distribution of feature values and density of class labels in the neighborhood is not considered. The randomly generated instances used for the approximations may not even be observed in real samples. A class of methods relies on extracting decision sets that depict the decision logic of the Machine Learning model in the form of conditional rules [37]. Extracting a subgroup of rules from the copious amounts of decision rule possibilities is deemed as an optimization problem with classification accuracy and overall interpretability as two main objectives [38]. As building inherently interpretable models for complex and high-accuracy tasks is a challenge, post-hoc methods are amongst the most important means of explainability of Machine Learning models.

Despite this wide variety of post-hoc methods for different data types and different output types, there is no evidence to show that they realize their intended outcome of helping the user understand the internals and decision logic of complex models. While these models are able to distill complex black-box models into simpler models and undemanding representations, whether these simplifications translate into users accurately understanding the internals and logic of the model is uncertain. For example, the human tendency to fill in the blanks can lead them to manufacture additional information which misconstrues the explanation [39], or the anchor effect can
hinder understanding when a misleading frame of reference is taken [40]. Thus, it is crucial to test the congruence between AI explanations and human understanding. In this paper, we test this on a very popular post-hoc method: Gradient-based saliency maps.

III. METHODOLOGY

A pre-trained model was used for the experiment: RoBERTa [31] that was trained on Stanford Sentiment Treebank [42]. The AllenNLP’s Interpret library was used to generate the model’s predictions and explanations [35] [43].

Subsequently, ten product reviews from e-commerce website Amazon [1] and restaurant reviews from travel review website Tripadvisor [2] were procured randomly, and then classified according to sentiment (positive or negative) using RoBERTa by AllenNLP. Based on the model card reported by AllenNLP [3], the model has achieved 95.11% accuracy in the test set, and hence, the predictions considered to be accurate. Subsequently, saliency map interpretations were generated for half of the predictions by visualising the gradient [44]. The text-specific class saliency maps highlighted the words in a given text that were discriminative with respect to the given class. These are post-hoc explanations to help users understand the top 5 words that helped RoBERTa in classifying the sentence into either negative or positive. An example of a review with top 5 discriminative words highlighted can be found in Figure 1. In order to reduce the complexity of the research and the top features were not, and were only highlighted without any specific order (as can be seen in [1]). This approach is very similar to the methodology in [45], although we did not get the idea from the mentioned paper directly, we are excited that both approaches are similar.

For the other half of the reviews, the words were highlighted at random instead of being based on the gradient. Keeping in mind that the randomly chosen word should not be one of the top-5 actual explanations. The simple gradient explanations and the ‘fabricated explanations’ – where the words were randomly highlighted – were shuffled and put into the questionnaire alongside the prediction from the RoBERTa binary classifier.

A survey was then created and distributed among 56 participants through email distribution lists. Figure [3] shows a screenshot of the survey’s first page. For each of the reviews, the survey-takers were requested to assess whether the highlighted words in the explanation strongly suggest alignment with the classification (positive or negative). You can see an example in [2] If post-hoc explanations are effective in this scenario, the survey takers should ideally agree with the predictions of all the sentences with the original saliency map. Additionally, survey-takers would be expected to disagree with the predictions of all the sentences with the words highlighted at random.

![Fig. 1. A negative classified review with top 5 discriminative words](image1.png)

![Fig. 2. Screenshot of first question](image2.png)

![Fig. 3. Screenshot of the survey](image3.png)

As the questionnaire comprised 10 questions, a point was
assigned to each question. If the participant was able to find out if the explanations were modified or not.

IV. RESULTS

On average, the participants achieved a score of 6.43 out of 10. Meaning that on average, only 6.43 out of 10 times the participants agreed with the prediction with the unmodified explanation and disagreed with the prediction with the modified explanation. Table I shows the statistics from the participation survey.

| Average | Median | Range | Mode |
|---------|--------|-------|------|
| 6.43 / 10 | 6 / 10 | 4 - 9 | 5 / 10 |

Table II shows the statistics of the responses to the predictions with unmodified simple gradient explanations. The points represent every time the survey taker agreed with an unmodified explanation’s prediction. The high average score shows that survey-takers were mainly aligned with the predictions and the top-weighted words for classifying the sentences with unmodified explanations. The agreement with the predictions is expected due to the aforementioned high accuracy of the model used. However, the conformity of the survey-takers with the highest weighted words is indicative of the explanations accurately depicting the words that would lead to the sentence’s classification. In other words, the simple gradient explanations in NLP are effective in helping end-users realise the most important features in predictions in a consumable form.

| Average | Median | Range | Mode |
|---------|--------|-------|------|
| 4.02 / 5 | 4 / 5 | 2 - 5 | 4 / 5 |

Table III shows the statistics of the responses to the predictions with modified simple explanations. The points represent every time the survey taker disagreed with a modified explanation’s prediction. The low average score indicates that the survey-takers often agreed with the randomised explanations justifying the respective prediction. This is counter to expectations, as the real highest-weighted discriminated words would often be missed, and words with low to negligible weights would often be highlighted as otherwise in the explanation. As such, these random words should not justify the prediction in most cases; however, the results show otherwise. We suspect that the participants draw improbable links between the explanations and the predictions. Seeing the false 'top-weighted words’ and the prediction, they perhaps come up with ways that they can justify the prediction, which influences their perception of the explanation. This can create a gap between the intended effect of explanations and the actual understanding of explanations by the end-users and developers. If true, the effect of this tendency can make end-users assess incorrect/unfair models as correct/fair. Furthermore, this casts doubt on the effectiveness of unmodified explanations. In that, high number of agreements with original explanation predictions by the participants might have been driven by this tendency and not the actual effectiveness of the explanation. However, more work is required to further explore this hypothesis and other ones that could underpin this discrepancy.

| Average | Median | Range | Mode |
|---------|--------|-------|------|
| 2.41 / 5 | 2 / 5 | 0 - 5 | 2 / 5 |

Figure 2 shows the instances of a question being answered by a participant in the form of a 'confusion matrix'. The quadrants are determined based on whether the question being answered pertained to a modified explanation or an original one, and whether the participant agreed with the prediction or disagreed. The concentration of instances in the 'Unmodified-Agree' quadrant and their sparseness in the 'Unmodified-Disagree' quadrant indicates that explanations are effective in justifying predictions through highlighting most important features. The instances in the 'Modified-Disagree' quadrant are expected since random explanations conventionally should not justify the predictions. However, the high number of observations in 'Modified-Agree' shows that the participants often agree with the predictions due to wrong reasons, and are fooled by the explanation in this scenario. This implies that simple gradients in NLP are not effective for people assessing the accuracy of a model or understanding the internals of it.

V. CONCLUSIONS

In this paper, we created a simple method to test the effectiveness of post-hoc explainability. The results of the survey indicate that simple gradient explanations in NLP are effective
in helping end-users realize the most important features in predictions in a consumable form. However, the survey also shows that the participants often agree with the predictions due to wrong reasons, and are fooled by the explanation in this scenario. This implies that simple gradients in NLP are not effective for people in assessing the accuracy of a model or understanding the internals of it. We can also conclude that current explainability methods that are based on gradients, specifically, simple gradients, might not clearly convey the reasons for the prediction to users. This will become more important as there is a need for trust and verifiability in models.

VI. FUTURE WORKS

For future work, we propose that there should be more exploration of verifiable and trustworthy model explanations where humans can judge whether they are correct or incorrect. Proposed future works include:

- More work on verifiable and trustworthy model explanations.
- A better way to provide decision support by using the natural language from the explanations.
- Combining multiple models and providing explanations for the multiple models together.
- Visualizing and using the explanations for debugging the models.
- Providing explanations for the fairness of models.

REFERENCES

[1] Y. Sahin, S. Bulkan, and E. Duman, “A cost-sensitive decision tree approach for fraud detection,” Expert Systems with Applications, vol. 40, no. 15, pp. 5916–5923, 2013.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” Advances in neural information processing systems, vol. 25, 2012.

[3] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” in 2009 IEEE conference on computer vision and pattern recognition. Ieee, 2009, pp. 248–255.

[4] T. Brown, B. Mann, N. Ryder, M. Subbiah, I. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell et al., “Language models are few-shot learners,” Advances in neural information processing systems, vol. 33, pp. 1877–1901, 2020.

[5] M. Shoeybi, M. Patwary, R. Puri, P. LeGresley, J. Casper, and B. Catanzaro, “Megatron-LM: Training multi-billion parameter language models using model parallelism,” arXiv preprint arXiv:1909.08055, 2019.

[6] R. Guidotti, A. Montele, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, “A survey of methods for explaining black box models,” ACM computing surveys (CSUR), vol. 51, no. 5, pp. 1–42, 2018.

[7] D. Pedreschi, S. Ruggieri, and F. Turini, “Discrimination-aware data mining,” in Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, 2008, pp. 560–568.

[8] F. Pasquale, The black box society: The secret algorithms that control money and information. Harvard University Press, 2015.

[9] A. Holzinger, G. Langs, H. Denk, K. Zatloukal, and H. Müller, “Causability and explainability of artificial intelligence in medicine,” Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 9, no. 4, p. e1312, 2019.

[10] B. Babic, S. Gerke, T. Evgeniou, and I. G. Cohen, “Beware explanations from ai in health care,” Science, vol. 373, no. 6552, pp. 284–286, 2021.

[11] B. Balaram, T. Greenham, and J. Leonard, “Engaging the public on automated decision systems,” in Artificial Intelligence: Real Public Engagement. Royal Society for the encouragement of Arts, Manufactures and Commerce, 2018.

[12] J. Larson, L. Mattu, S. Kirchner, and J. Angwin, “How we analyzed the compas recidivism algorithm,” ProPublica, 2016.

[13] F. Xu, H. Uszkoreit, Y. Du, W. Fan, D. Zhao, and J. Zhu, “Explainable ai: A brief survey on history, research areas, approaches and challenges,” in CCF international conference on natural language processing and Chinese computing, Springer, 2019, pp. 563–574.

[14] A. C. Scott, W. J. Clancey, R. Davis, and E. H. Shortliffe, “Explanation capabilities of production-based consultation systems,” STANFORD UNIV CA DEPT OF COMPUTER SCIENCE, Tech. Rep., 1977.

[15] K. Dzugaite, S. Ben-David, and D. Roy, “Enforcing interpretability and its statistical impacts: Trade-offs between accuracy and interpretability,” arXiv, 2020.

[16] E. M. Kenny, E. D. Delaney, D. Greene, and M. T. Keane, “Post-hoc explanation options for xai in deep learning: The insight centre for data analytics perspective,” in International Conference on Pattern Recognition. Springer, 2021, pp. 20–34.

[17] H. Hagras, “Toward human-understandable, explainable ai,” Computer, vol. 51, no. 9, pp. 28–36, 2018.

[18] C. Mallavarapu, R. Mandalav, S. KC, and G. Holt, “Political profiling using feature engineering and nlp,” SMU Data Science Review, 2018.

[19] A. Blais, E. Gedigeng, and N. Nevitte, “Do polls influence the vote?” The University of Michigan Press.

[20] D. Ramesh and S. Sanampudi, “An automated essay scoring systems: a systematic literature review,” in Artificial Intelligence Review, 2022, pp. 245–257.

[21] G. Montavon, W. Samek, and K.-R. Müller, “Methods for interpreting and understanding deep neural networks,” Digital signal processing, vol. 73, pp. 1–15, 2018.

[22] J. R. Quinlan, “Induction of decision trees,” Machine learning, vol. 1, no. 1, pp. 81–106, 1986.

[23] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” nature, vol. 521, no. 7553, pp. 436–444, 2015.

[24] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” Neural computation, vol. 9, no. 8, pp. 1735–1780, 1997.

[25] S. Sachan, F. Almaghrabi, J.-B. Yang, and D.-L. Xu, “Evidential reasoning for preprocessing uncertain categorical data for trustworthy decisions: An application on healthcare and finance,” Expert Systems with Applications, vol. 185, p. 115597, 2021.

[26] D. Gunning, “Explainable artificial intelligence (xai),” Defense advanced research projects agency (DARPA), nd Web, vol. 2, no. 2, p. 1, 2017.

[27] W. Samek, T. Wiegand, and K.-R. Müller, “Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models,” arXiv preprint arXiv:1708.08296, 2017.

[28] S. Tan, R. Caruana, G. Hooker, and Y. Lou, “Distill-and-compare: Auditing black-box models using transparent model distillation,” in Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, 2018, pp. 303–310.

[29] S. Chandler, “How explainable ai is helping algorithms avoid bias,” Forbes, 2020.

[30] S. M. Lundberg, G. Erion, H. Chen, A. DeGrave, J. M. Prutkin, B. Nair, R. Katz, J. Himmelfarb, N. Bansal, and S.-I. Lee, “From local explanations to global understanding with explainable ai for trees,” Nature machine intelligence, vol. 2, no. 1, pp. 56–67, 2020.

[31] S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” in Advances in Neural Information Processing Systems 30, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates, Inc., 2017, pp. 4765–4774. [Online]. Available: http://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions.pdf

[32] M. F. Ribeiro, S. Singh, and C. Guestrin, “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.

[33] A. Shrikumar, P. Greenside, and A. Kundaje, “Learning important features through propagating activation differences,” in International conference on machine learning. PMLR, 2017, pp. 3145–3153.

[34] H. Nori, S. Jenkins, P. Koch, and R. Caruana, “Interpretml: A unified framework for machine learning interpretability,” arXiv preprint arXiv:1909.09223, 2019.

[35] E. Wallace, J. Tuyls, J. Wang, S. Subramanian, M. Gardner, and S. Singh, “Allenlp interpret: Explaining predictions of nlp models.”

[36] D. Slack, S. Hilgard, S. Singh, and H. Lakkaraju, “Fooling lime with Applications,” PMLR, 2017, pp. 3145–3153.
[37] L. Himabindu, E. Kamar, R. Caruana, and J. Leskovec, “Interpretable & explorable approximations of black box models,” in arXiv preprint arXiv:1707.01154, 2017.

[38] L. Himabindu, S. Bach, and J. Leskovec, “Interpretable decision sets: A joint framework for description and prediction,” in 22nd ACM SIGKDD international conference on knowledge discovery and data mining, 2016, pp. 1675–1684.

[39] L. Freeman, “Filling in the blanks: A theory of cognitive categories and the structure of social affiliation,” Social Psychology Quarterly, pp. 118–127, 1992.

[40] A. Furnham, “A literature review of the anchoring effect,” The journal of socio-economics 40, pp. 35–42, 2011.

[41] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, “Roberta: A robustly optimized bert pretraining approach,” arXiv preprint arXiv:1907.11692, 2019.

[42] R. Socher, A. Perelygin, J. Wu, J. Chuang, C. D. Manning, A. Y. Ng, and C. Potts, “Recursive deep models for semantic compositionality over a sentiment treebank,” in Proceedings of the 2013 conference on empirical methods in natural language processing, 2013, pp. 1631–1642.

[43] M. Gardner, J. Grus, M. Neumann, O. Tafjord, P. Dasigi, N. Liu, M. Peters, M. Schmitz, and L. Zettlemoyer, “Allennlp: A deep semantic natural language processing platform,” arXiv preprint arXiv:1803.07640, 2018.

[44] K. Simonyan, A. Vedaldi, and A. Zisserman, “Deep inside convolutional networks: Visualising image classification models and saliency maps,” arXiv preprint arXiv:1312.6034, 2013.

[45] H. Schuff, A. Jacovi, H. Adel, Y. Goldberg, and N. T. Vu, “Human interpretation of saliency-based explanation over text,” arXiv preprint arXiv:2201.11569, 2022.