Abstract

Saliency map generation techniques are at the forefront of explainable AI literature for a broad range of machine learning applications. Our goal is to question the limits of these approaches on more complex tasks. In this paper we apply Layer-Wise Relevance Propagation (LRP) to a sequence-to-sequence attention model trained on a text summarization dataset. We obtain unexpected saliency maps and discuss the rightfulness of these “explanations”. We argue that we need a quantitative way of testing the counterfactual case to judge the truthfulness of the saliency maps. We suggest a protocol to check the validity of the importance attributed to the input and show that the saliency maps obtained sometimes capture the real use of the input features by the network, and sometimes do not. We use this example to discuss how careful we need to be when accepting them as explanation.

1 Introduction

Ever since the LIME algorithm [Ribeiro et al., 2016], “explanation” techniques focusing on finding the importance of input features in regard of a specific prediction have soared and now have many ways of finding saliency maps (also called heat-maps because of the way we like to visualize them). We are interested in this paper by the use of such a technique in an extreme task that highlights questions about the validity and evaluation of the approach. We would like to first set the vocabulary we will use. We agree that saliency maps are not explanations in themselves and that they are more similar to attribution, which is only one part of the human explanation process [Miller, 2019]. We will prefer to call this importance mapping of the input an attribution rather than an explanation. We will talk about the importance of the input relevance score in regard to the model’s computation and not make allusion to any human understanding of the model as a result.

There exist multiple ways to generate saliency maps over the input for non-linear classifiers [Bach et al., 2015; Montavon et al., 2017; Samek et al., 2017]. We refer the reader to [Adadi and Berrada, 2018] for a survey of explainable AI in general. We use in this paper Layer-Wise Relevance Propagation (LRP) [Bach et al., 2015] which aims at redistributing the value of the classifying function on the input to obtain the importance attribution. It was first created to “explain” the classification of neural networks on image recognition tasks. It was later successfully applied to text using convolutional neural networks (CNN) [Arras et al., 2017a] and then Long-Short Term Memory (LSTM) networks for sentiment analysis [Arras et al., 2017b].

Our goal in this paper is to test the limits of the use of such a technique for more complex tasks, where the notion of input importance might not be as simple as in topic classification or sentiment analysis. We changed from a classification task to a generative task and chose a more complex one than text translation (in which we can easily find a word to word correspondence/importance between input and output). We chose text summarization. We consider abstractive and informative text summarization, meaning that we write a summary “in our own words” and retain the important information of the original text. We refer the reader to [Radev et al., 2002] for more details on the task and the different variants that exist. Since the success of deep sequence-to-sequence models for text translation [Bahdanau et al., 2014], the same approaches have been applied to text summarization tasks [Rush et al., 2015; See et al., 2017; Nallapati et al., 2016] which use architectures on which we can apply LRP.

We obtain one saliency map for each word in the generated summaries, supposed to represent the use of the input features for each element of the output sequence. We observe that all the saliency maps for a text are nearly identical and decorrelated with the attention distribution. We propose a way to check their validity by creating what could be seen as a counterfactual experiment from a synthesis of the saliency maps, using the same technique as in Arras et al. [2017b]. We show that in some but not all cases they help identify the important input features and that we need to rigorously check importance attributions before trusting them, regardless of whether or not the mapping “makes sense” to us. We finally argue that in the process of identifying the important input features, verifying the saliency maps is as important as the generation step, if not more.

2 The Task and the Model

We present in this section the baseline model from See et al. [2017] trained on the CNN/Daily Mail dataset. We reproduce the results from See et al. [2017] to then apply LRP on it.
3.1 Mathematical Description

We initialize the relevance of the output layer to the value of the predicted class before softmax and then describe locally the propagation backwards of the relevance from layer to layer. For normal neural network layers we use the form of LRP with epsilon stabilizer [Bach et al., 2015]. We write down $R_{i,j}^{l+1}$ the relevance received by the neuron $i$ of layer $l$ from the neuron $j$ of layer $l+1$:

$$R_{i,j}^{l+1} = \frac{w_{i,j}^{l+1} z_j^l + \epsilon \text{ sign} (z_j^{l+1}) + b_j^{l+1}}{z_j^{l+1} + \epsilon \text{ sign} (z_j^{l+1})} * R_{i,j}^{l+1} \quad (1)$$

where $w_{i,j}^{l+1}$ is the network’s weight parameter set during training, $b_j^{l+1}$ is the bias for neuron $j$ of layer $l + 1$, $z_j^l$ is the activation of neuron $i$ on layer $l$, $\epsilon$ is the stabilizing term set to 0.00001 and $D_l$ is the dimension of the $l$-th layer.

The relevance of a neuron is then computed as the sum of the relevance he received from the above layer(s).

For LSTM cells we use the method from Arras et al.[2017b] to solve the problem posed by the element-wise multiplications of vectors. Arras et al. noted that when such computation happened inside an LSTM cell, it always involved a “gate” vector and another vector containing information. The gate vector containing only value between 0 and 1 is essentially filtering the second vector to allow the passing of “relevant” information. Considering this, when we propagate relevance through an element-wise multiplication operation, we give all the upper-layer’s relevance to the “information” vector and none to the “gate” vector.

3.2 Generation of the Saliency Maps

We use the same method to transmit relevance through the attention mechanism back to the encoder because Bahdanau’s attention [Bahdanau et al., 2014] uses element-wise multiplications as well. We depict in Figure 2 the transmission end-to-end from the output layer to the input through the decoder, attention mechanism and then the bidirectional encoder. We then sum up the relevance on the word embedding to get the token’s relevance as Arras et al. [2017b].

The way we generate saliency maps differs a bit from the usual context in which LRP is used as we essentially don’t
have one classification, but 200 (one for each word in the summary). We generate a relevance attribution for the 50 first words of the generated summary as after this point they often repeat themselves.

This means that for each text we obtain 50 different saliency maps, each one supposed to represent the relevance of the input for a specific generated word in the summary.

4 Experimental results

In this section, we present our results from extracting attributions from the sequence-to-sequence model trained for abstractive text summarization. We first have to discuss the difference between the 50 different saliency maps we obtain and then we propose a protocol to validate the mappings.

4.1 First Observations

The first observation that is made is that for one text, the 50 saliency maps are almost identical. Indeed each mapping highlights mainly the same input words with only slight variations of importance. We can see in Figure 3 an example of two nearly identical attributions for two distant and unrelated words of the summary. The saliency map generated using LRP is also uncorrelated with the attention distribution that participated in the generation of the output word. The attention distribution changes drastically between the words in the generated summary while not impacting significantly the attribution over the input text. We deleted in an experiment the relevance propagated through the attention mechanism to the encoder and didn’t observe much changes in the saliency map.

It can be seen as evidence that using the attention distribution as an “explanation” of the prediction can be misleading. Quantifying the difference between attention distribution and saliency map across multiple tasks is a possible future work.

The second observation we can make is that the saliency map doesn’t seem to highlight the right things in the input for the summary it generates. The saliency maps on Figure 3 correspond to the summary from Figure 1, and we don’t see the word “video” highlighted in the input text, which seems to be important for the output.

This allows us to question how good the saliency maps are in the sense that we question how well they actually represent the network’s use of the input features. We will call that truthfulness of the attribution in regard to the computation, meaning that an attribution is truthful in regard to the computation if it actually highlights the important input features that the network attended to during prediction. We proceed to measure the truthfulness of the attributions by validating them quantitatively.
4.2 Validating the Attributions

We propose to validate the saliency maps in a similar way as Arras et al. [2017b] by incrementally deleting “important” words from the input text and observe the change in the resulting generated summaries.

We first define what “important” (and “unimportant”) input words mean across the 50 saliency maps per texts. Relevance transmitted by LRP being positive or negative, we average the absolute value of the relevance across the saliency maps to obtain one ranking of the most “relevant” words. The idea is that input words with negative relevance have an impact on the resulting generated word, even if it is not participating positively, while a word with a relevance close to zero should not be important at all. We did however also try with different methods, like averaging the raw relevance or averaging a scaled absolute value where negative relevance is scaled down by a constant factor. The absolute value average seemed to deliver the best results.

We delete incrementally the important words (words with the highest average) in the input and compared it to the control experiment that consists of deleting the least important word and compare the degradation of the resulting summaries. We obtain mitigated results: for some texts, we observe a quick degradation when deleting important words which are not observed when deleting unimportant words (see Figure 4), but for other test examples we don’t observe a significant difference between the two settings (see Figure 5).

![Deleting 7% most important words: the <UNK> mass index was carried out against the taliban in 2012. the <UNK> mass index was part of china’s ‘strike hard’ campaign against the notion that the mid-1970s was killed[truncated]](image)

![Deleting 7% least important words: the <UNK> mass index was carried out in the wake of the horrific attack on a school in peshawar. the government has issued a ban on executions in the country[truncated]](image)

Figure 4: Summary from Figure 1 generated after deleting important and unimportant words from the input text. We observe a significant difference in summary degradation between the two experiments, where the decoder just repeats the UNKNOWN token over and over.

One might argue that the second summary in Figure 5 is better than the first one as it makes better sentences but as the model generates inaccurate summaries, we do not wish to make such a statement.

This however allows us to say that the attribution generated for the text at the origin of the summaries in Figure 4 are truthful in regard to the network’s computation and we may use it for further studies of the example, whereas for the text at the origin of Figure 5 we shouldn’t draw any further conclusions from the attribution generated.

One interesting point is that one saliency map didn’t look “better” than the other, meaning that there is no apparent way of determining their truthfulness in regard of the computation without doing a quantitative validation. This brings us to believe that even in simpler tasks, the saliency maps might make sense to us (for example highlighting the animal in an image classification task), without actually representing what the network really attended too, or in what way.

We defined without saying it the counterfactual case in our experiment: “Would the important words in the input be deleted, we would have a different summary”. Such counterfactuals are however more difficult to define for image classification for example, where it could be applying a mask over an image, or just filtering a colour or a pattern. We believe that defining a counterfactual and testing it allows us to measure and evaluate the truthfulness of the attributions and thus weight how much we can trust them.

5 Conclusion

In this work, we have implemented and applied LRP to a sequence-to-sequence model trained on a more complex task than usual: text summarization. We used previous work to solve the difficulties posed by LRP in LSTM cells and adapted the same technique for Bahdanau et al. [2014] attention mechanism.

We observed a peculiar behaviour of the saliency maps for the words in the output summary: they are almost all identical and seem uncorrelated with the attention distribution. We then proceeded to validate our attributions by averaging the absolute value of the relevance across the saliency maps. We obtain a ranking of the word from the most important to the least important and proceeded to delete one or another.

We showed that in some cases the saliency maps are truthful to the network’s computation, meaning that they do highlight the input features that the network focused on. But we also showed that in some cases the saliency maps seem to not capture the important input features. This brought us to discuss the fact that these attributions are not sufficient by themselves, and that we need to define the counter-factual case and test it to measure how truthful the saliency maps are.

Future work would look into the saliency maps generated by applying LRP to pointer-generator networks and compare to our current results as well as mathematically justifying the average that we did when validating our saliency maps. Some additional work is also needed on the validation of the saliency maps with counterfactual tests. The exploitation and evaluation of saliency map are a very important step and should not be overlooked.
References

[Adadi and Berrada, 2018] Amina Adadi and Mohammed Berrada. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, 6:52138–52160, 2018.

[Arras et al., 2017a] Leila Arras, Franziska Horn, Grégoire Montavon, Klaus Robert Müller, and Wojciech Samek. "What is relevant in a text document?": An interpretable machine learning approach. *PLoS ONE*, 12(8):1–19, 2017.

[Arras et al., 2017b] Leila Arras, Grégoire Montavon, Klaus-Robert Müller, and Wojciech Samek. Explaining Recurrent Neural Network Predictions in Sentiment Analysis. 2017.

[Bach et al., 2015] Sebastian Bach, Alexander Binder, Grégoire Montavon, Frederick Klauschen, Klaus Robert Müller, and Wojciech Samek. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. *PLoS ONE*, 10(7):1–46, 2015.

[Bahdanau et al., 2014] Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio. Neural Machine Translation by Jointly Learning to Align and Translate. *arXiv preprint arXiv:1409.0473*, 2014.

[Hochreiter and Schmidhuber, 1997] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.

[Miller, 2019] Tim Miller. Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, 267:1–38, 2019.

[Montavon et al., 2017] Grégoire Montavon, Wojciech Samek, and Klaus-Robert Müller. Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73:1–15, feb 2017.

[Nallapati et al., 2016] Ramesh Nallapati, Bowen Zhou, Cicero Nogueira dos Santos, Caglar Gulcehre, and Bing Xiang. Abstractive Text Summarization Using Sequence-to-Sequence RNNs and Beyond. *arXiv preprint arXiv:1602.06023*, 2016.

[Radev et al., 2002] Dragomir R. Radev, Eduard Hovy, and Kathleen McKeown. Introduction to the Special Issue on Summarization. *Computational Linguistics*, 28(4):399–408, 2002.

[Ribeiro et al., 2016] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1135–1144, 2016.

[Rush et al., 2015] Alexander M Rush, Sumit Chopra, and Jason Weston. A Neural Attention Model for Abstractive Sentence Summarization. *arXiv preprint arXiv:1509.00685*, sep 2015.

[Samek et al., 2017] Wojciech Samek, Alexander Binder, Grégoire Montavon, Sebastian Lapuschkin, and Klaus Robert Müller. Evaluating the visualization of what a deep neural network has learned. *IEEE Transactions on Neural Networks and Learning Systems*, 28(11):2660–2673, 2017.

[See et al., 2017] Abigail See, Peter J Liu, and Christopher D Manning. Get to the point: Summarization with pointer-generator networks. *arXiv preprint arXiv:1704.04368*, 2017.