Reducing Hallucinations in Neural Machine Translation with Feature Attribution

Joël Tang  
Imperial College London  
joel.tang20@imperial.ac.uk

Marina Fomicheva  
University of Sheffield  
m.fomicheva@sheffield.ac.uk

Lucia Specia  
Imperial College London  
l.specia@imperial.ac.uk

Abstract

Neural conditional language generation models achieve the state-of-the-art in Neural Machine Translation (NMT) but are highly dependent on the quality of parallel training dataset. When trained on low-quality datasets, these models are prone to various error types, including hallucinations, i.e. outputs that are fluent, but unrelated to the source sentences. These errors are particularly dangerous, because on the surface the translation can be perceived as a correct output, especially if the reader does not understand the source language. We present a case study focusing on model understanding and regularisation to reduce hallucinations in NMT. We first use feature attribution methods to study the behaviour of an NMT model that produces hallucinations. We then leverage these methods to propose a novel loss function that substantially helps reduce hallucinations and does not require retraining the model from scratch.

1 Introduction

Despite impressive progress in Machine Translation (MT) with neural approaches (Bahdanau et al., 2014; Vaswani et al., 2017), translation adequacy, i.e. the preservation of the source meaning in the translated sentence, still constitutes an issue in current models (Castilho et al., 2017; Sharou and Specia, 2022). In particular, such systems may “hallucinate” content, i.e. generate outputs that read fluently in the target language, but are completely unrelated to the source sentences (Müller et al., 2020; Raunak et al., 2021). These errors are particularly dangerous as they can go unnoticed by the end user of MT if they do not speak the source language.

While there has been substantial work on improving NMT quality in general, very few previous studies have looked specifically at hallucinations. Some propose an auxiliary loss to encourage unlikely generations from the decoder to receive lower probability (Welleck et al., 2019). However, they only address a specific type of hallucinations, namely repeated n-grams. Other studies have addressed under-translation and over-translation (Tu et al., 2016; Garg et al., 2019), which are related linguistic phenomena but do not necessarily correspond to hallucinations: under-translation refers to non-translated words, and over-translation refers to words translated multiple times.

Recent work has observed that, when hallucinating, neural MT models tend to over-rely on the generated target tokens and ignore the source sentence (Voita et al., 2021). In this paper, we analyse the behaviour of a neural MT model on hallucinated instances wrt both source and target tokens using a feature attribution method (Sundararajan et al., 2017; Schulz et al., 2020). Feature attribution methods assign relevance scores to source and target input tokens according to their contribution to the generated output. We observe that a distinctive characteristic of the hallucinated instances is a high entropy of feature attribution scores assigned to the source sentence. Based on this analysis, we devise an auxiliary loss to reduce the amount of hallucinations in MT output. Our experiments show that this loss function successfully mitigates the observed hallucinations.
2 Data

For our experiments, we use the MLQE-PE dataset (Fomicheva et al., 2020), which provides manual quality assessments on a continuous [0..100] scale (Direct Assessment – DA) for 10,000 sentences per language and access to the neural MT models used to generate the translations (a strong fairseq Transformer model). As suggested in previous related work (Specia et al., 2021), this dataset has a high percentage of hallucinated sentences for the Romanian-English (Ro-En) language pair, which was trained on noisier data. We focus on this language pair in our experiments.

The dataset does not include manual annotation for hallucinations. We use DA scores as a proxy for selecting hallucinated sentences. Based on the annotation guidelines, we select two subsets: translations with score lower than 25 (lowest quality band) are labelled as containing hallucinations, and translations with scores above 85 (highest quality band) are labelled as not containing hallucinations. The resulting dataset contains 567 hallucinated and 3,134 non-hallucinating sentences.

Manual inspection of a sample of sentences with DA scores lower than 25 confirms a clear hallucinating behaviour. Table 1 provides examples of hallucinations of various types, including fully detached sentences that do not have anything in common with the source sentence, oscillatory hallucinations that consist in repeated n-grams (Raunak et al., 2021), as well as mixed cases.

3 Analysis

First, we look at the input patterns that induce hallucinations. Second, we use feature attribution to gain insight into model behaviour on hallucinated sentences.

3.1 Hallucination Triggers

Manual inspection of hallucinated sentences in our dataset shows that hallucinations are often caused by the model’s lack of robustness given specific inputs. In particular, the model is very sensitive to rare/unknown tokens, such as out-of-vocabulary (OOV) tokens. Figure 1 illustrates this phenomenon: we observe a strong correlation between the presence of at least one OOV token and the hallucination phenomenon, based on the analysis of DA scores. The set of source sentences containing at least one OOV token shows the lowest translation quality scores.

Having identified this weakness in the model, we wanted to test if by simulating OOV tokens we could induce hallucinations. For that, we introduce an out-of-vocabulary token (UNK) in different positions in a subset of 200 sentences with a translation quality score $\geq 85$, i.e., clean sentences (without OOV and correctly translated before). For comparison, we perturb the same set of sentences with a commonly used token in the same positions. The results are shown in Figure 2 for the hallucinating Ro-En model, and in Figure 3 for a non-hallucinating Estonian-English (Et-En) model. We use BLEU score as a proxy for measuring the degraded quality, in comparison to the reference output (which is the correct translation without any alteration). Perturbations with UNK token have a very strong impact on translation quality. Interestingly, the impact decreases as the token is inserted later in the sentence. In comparison, a perturbation with a commonly used token is less likely to lead to hallucinations. This shows the lack of robustness to rare words in the translation model, which leads to hallucination. In comparison, the Et-En model, under the same

| Type       | Example                                                                 | Source                                                                                                                                  | Correct Translation                                                                 | Model output                                                                                   |
|------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Oscillatory| Source: 1936—a făcut apel în justiție contra falsificatorilor operei sale. | Correct Translation: 1936 - filed a lawsuit against the forgers of his work.                                                          | Model output: B6 - B6 - B6 - B6 - B6 - B6 - B6                                         |
| Detached   | Source: In iulie 1996, jurnalista Ludmila Gorbul fondează publicatia periodică de limba română “Cugetul” | Correct Translation: In July 1996, the journalist Ludmila Gorbul founded regular publication on Romanian language.                 | Model output: The second subparagraph of Article 6 (1) (c) of Directive 2000 / 29 / EC is to apply. |
| Mixed      | Source: Un obicei curent al locuitorilor din Livadia era legat de trenurile personale, care traversau satul și de oprirea lor la halta C.F.R. | Correct Translation: A common custom of the inhabitants of Livadia was related to personal trains, which crossed the village and to their stop at the C.F.R. | Model output: Primary Copper Smelters - 40 C.F.R. Part 63, Subpart FFFFFFFFFFFFFF;          |

Table 1: Examples of hallucination from the MLQE-PE dataset for the Romanian-English language pair.
Figure 1: Orange: count of instances containing at least one OOV token in the source sentence. Blue: instances containing no OOV tokens in the source sentence. z-mean is the averaged standardised z-score across multiple annotators for a given sentence.

Figure 2: Ro-En model. Blue: inserting an in-vocabulary and frequent random token ("e"); orange: inserting the UNK token.

OOV perturbation, is much more robust, as the altered BLEU score is lower-bounded by 50 instead of 30 for the Ro-En model.

3.2 Feature Attribution

Here we study the link between feature attribution scores and the hallucinating behaviour. Feature attribution scores are scalar metrics reflecting the importance of a given input feature for the model prediction. These scores have no ground truth, and are often used as a proxy for model understanding.

We chose Integrated Gradients (Sundararajan et al., 2017) as our feature attribution method, as it has been shown effective for other tasks. This method is inspired by the Input*Gradients approach, which takes the signed partial derivatives of the output with respect to the input and multiplies them by the input itself. The Integrated Gradients method improves on this by aggregating the gradients along a path from an uninformative baseline input to the actual input: we chose the uninformative baseline to be completely an empty padded source sentence and an empty padded prefix (with only a BOS token), conveying no information. We chose this method as it has been shown to be effective, easy to interpret, and differentiable, which is a strong requirement as we later devise a training loss function based on it.

NMT with Transformers is modelled as an autoregressive task, where each translated token is generated in order. At each generation step, the whole source sentence and all the previously translated tokens are available as inputs to the model. At each time step, we compute attribution scores for each token in the target prefix and in the source. The scores are computed using a sum aggregation over the dimensions of the token embedding.

To investigate whether there are any distinctive patterns in model attributions that would characterise hallucinations, we train an XGBoost classifier to predict if a token (after tokenization and BPE) is hallucinated or not, using a set of features based on the attributions scores: entropy of attributions scores across source tokens, entropy of attributions scores across target tokens and attribution gradients (ignoring padded tokens) relative to the current timestep: at timestep $i$, we analyse the tokens $t_i, t_{i-1}, ..., t_0$ and $s_0, ..., s_{\text{len}(s)}$. Intuitively, we expect an adequate translation to exhibit lower entropy on source attributions with a few source tokens (corresponding to the current target token) having high relevance scores.

Given the lack of datasets with natural hallucinations explicitly annotated at token level, we use our sentence-level dataset (Section 2) with a simplifying assumption that all tokens in the hallucinated sentences are labelled as hallucinated. We
obtain a validation F1-score of 0.61. Early stopping was used on a distinct validation dataset, with 15 estimators, a max depth of 6, row and columns subsampling ratio of 0.8, minimum child weight of 3.0, lambda and alpha regularization of 1. These parameters were found through randomised grid search, with three values per parameter. Table 2 shows examples of the predictions of the classifier. We observe a strong relationship between the predictions of the classifier and the hallucinating behaviour. False positives token-level classifications often include tokens ending a word, frequent tokens, and conjunction tokens: for instance, the year 1945, frequent tokens such as at, the (in red: wrongly classified as hallucinated). It is probable that these tokens are generated with over-reliance on the target prefixes.

4 Loss Function

Table 3 shows the mean values of four features defined in Section 3.2 on the two subsets of our validation set (correct and hallucinated). Gradients is the numerical gradient of the normalised non-zero attributions as a function of the timestep. We then sum the absolute values.

Overall, the mean values are higher for hallucinated tokens, except for attribution gradients on the target prefix. The most discriminative feature seems to be the entropy of attribution values on the source tokens. Based on this observation, we propose the following learning objective for MT training:

$$\mathcal{L} = \mathcal{L}_{CE} + \lambda \mathcal{L}_{Attr}$$  \hspace{1cm} (1)

where $\mathcal{L}_{CE}$ is the standard cross-entropy (CE) loss with label smoothing, and $\mathcal{L}_{Attr}$ is the proposed attribution-based loss. We define $\mathcal{L}_{Attr}$ as the entropy of the attribution values on the source tokens averaged across generation time steps:

$$\mathcal{L}_{Attr} = \mathcal{H}[IG^*(X_{source})]$$  \hspace{1cm} (2)

where $IG^*$ corresponds to the Integrated Gradients attribution method. This method has a prohibitive computational complexity to be used at training time for a generation task. To reduce computational complexity, we use an approximation, with only one step in the comparison between the input and the baseline representation:

$$IG^*_i(x) := (x_i - x'_i) \frac{\partial F(x)}{\partial x_i}$$  \hspace{1cm} (3)

with $x_i$ being the input, $x'_i$ the uninformative baseline input (empty source sentence and BOS target sentence) and $F$ the model function. $x'_i$ is the vector generated by the following sequences of tokens: $T_{source} = ([PAD], ...,[PAD])$ and $T_{prefix} = ([BOS],[PAD],...,[PAD])$.

Teaching the model to decrease the entropy of the source attributions is justified by the statistics shown in Table 3 as this value is lower for non-hallucinated sentences. Moreover, it also encourages the model the narrow the focus on tokens, hence making the influence of perturbation tokens less important along the entire sentence, as in the perturbations experiments in Section 3.

To test whether our method reduces the amount of hallucinated sentences, we fine-tune the base Ro-En translation model using the proposed auxiliary loss. For comparison we keep training the base model with the standard CE loss under the same process: same hyper-parameters and early stopping. We used Adam as optimiser, the learning rate was set to continue from the last epoch before fine-tuning, the scheduler was reset (inverse square root), weight decay was set to 10e-4, label smoothing weight to 0.1 and dropout ratio to 0.3. The maximum number of epochs was set to 30. The model was trained with the fairseq library, same as the base model. We set the weight of our loss to 5 (versus 1 for the cross-entropy): this was to keep the same order of magnitude between the two values during training.

We evaluate the performance of the models on the full Ro-En MLQE-PE dataset, as well as specifically on the hallucinated and non-hallucinated subsets. Since the dataset does not provide reference translations, we back-translate the generated English MT outputs into Romanian using Google Translate API and compute BLEU score between the back-translated Romanian sentences and the original source sentences from the dataset.

Table 4 shows the results. We observe a very strong improvement of almost 10 BLEU points from fine-tuning with the proposed loss on the entire test set (Overall - 7,000 sentences). The improvement is even more evident for the set of source sentences with the lowest initial translation quality, which we hypothesised was due to a high incidence of hallucinations (Halluc.). The fine-tuned model with our additional loss successfully mitigates the hallucination behaviour, compared to
Bill that the Bill is to be passed, and then the Bill is to be passed, as it is referred to as an Bill.

It shall immediately submit, on simple request by the Commission, information on the measures already taken and planned to comply with this Decision.

Nour re dine is the main contributor of the oil and gas industries in the DPRK.

The applicant claims that the environmental impact of the tourist accommodation is not limited to the overall environmental impact of the tourist accommodation.

In the event of a failure to meet the requirement of point 1.1.2.1, the Ducks concerned have not been brought forward in the course of the formal investigation procedure.

B one - off waste (B B B C): half - scale (B B B C) B 6: B 6: B 6: B 6: B 6: B 6: B 6: B 6:

The second subparagraph is to adopt the basic basic criteria which are to be met by the second stage.

B 6 - B 6 - B 6 - B 6 - B 6

B one - off one - off - one - that was then another was the Bill.

After 1945, decolonisation is taking place and Europe is divided between the spheres of the US and the US SR.

In Congresss Henry Clay was at the forefront of an effort to re-authorise.

This massive change has made accumulation and exchange of experience impossible.

The magnitude of statistical death depends on the number of people affected by the counter measure.

These focused attacks should have destroyed the Serbian army at the heart of the country.

An na and Do sto iv ski are first established in Berlin, then moved to Dresden.

The population of Malta was estimated at 408,000 in July 2011.

III. / J G1 has also lost at least two F w 190 for the same reason.

Benito Mussolini was killed by Italian parti sans on 28 April.

In June 1944 only 50,800 t had been produced compared with 180,000 t planned.

The event attracted six million visitors within five months.

The risks and opportunities for the peaceful use of nuclear energy have been discussed and have caused controversy.

German civilian morals were not a primary objective for USAF planners.

Table 2: Hallucinated (top) and non-hallucinated (bottom) translations. The tokens predicted as hallucinations by the token-level binary classifier are marked in red.

| Source | Correct | Hallucinated |
|--------|---------|--------------|
| S attr. entropy | 3.51±0.52 | 3.91±0.50 |
| T attr. entropy | 1.73±0.99 | 2.47±1.15 |
| S att. gradients | 0.92±0.22 | 1.01±0.22 |
| T att. gradients | 0.74±0.33 | 0.74±0.32 |

Table 3: Entropy and gradients of the attribution scores for Source (S) and Target (T) for the hallucinated and correct translations in our dataset. Mean and standard deviation are computed for each portion of the dataset (completely correct and completely hallucinated).

Table 4: BLEU scores of the model fine-tuned with the proposed auxiliary loss compared to the base model on different subsets of data.

| Model | Overall | Halluc. | Non-Halluc. |
|-------|---------|---------|-------------|
| Baseline | 28.90 | 10.71 | 35.29 |
| Fine-tuned | 38.25 | 24.46 | 44.90 |

Table 5: Example of hallucinated MT output by the base model and the improved version by our model.

| Source | In iulie 1996, jurnalista Ludmila Gorbil fundă publicația periodică de limba română “Cugetul” |
|--------|------------------------------------------------------------------|
| Base model | (RO) Mr President, in July 1996, the official Ludmila Gorbil founded the regular publication of the Romanian language, which was published in the Official Journal of the European Union. |
| Our model | In July 1996, the journalist Ludmila Gorbil founded regular publication on Romanian language. |
outputs that would have been correct without the additional loss function. In particular, despite the presence of an OOV token (the first quotation mark in the source sentence), our model successfully recovers the main meaning of the source sentence in its translation, even if the coverage is partial (the word "Cugetul" is missing).

5 Conclusions

Our work studies the hallucinations phenomenon on a Romanian-to-English translation model, using a standard Transformer architecture. First, we analysed the observed hallucinations in order to understand potential triggers that let to them. We showed that specific patterns from the source sentence could induce hallucinations, which is an interesting take on the hallucination problem from a data/model robustness perspective. Then, we studied the behaviour of the hallucinating model using feature attribution methods to investigate whether this behaviour can be quantified in a differentiable way that could be used to inform the design of new loss functions for better model training. We found that the entropy of the attribution values on the source tokens is effective at discriminating hallucinating from non-hallucinating tokens. Based on these findings, we proposed a novel and intuitive loss function that successfully increases the robustness of the model to the observed trigger patterns and hence decreases hallucinations occurrences.

In future work, we plan to study whether our approach generalises to other language pairs and hallucinations caused by other triggers.

References

[Bahdanau et al.2014] Bahdanau, Dzmitry, Kyunghyun Cho, and Yoshua Bengio. 2014. Neural machine translation by jointly learning to align and translate. arXiv preprint arXiv:1409.0473.

[Castilho et al.2017] Castilho, Sheila, Joss Moorkens, Federico Gaspari, Jacer Calixto, John Tinsley, and Andy Way. 2017. Is neural machine translation the new state of the art? The Prague Bulletin of Mathematical Linguistics, (108).

[Fomicheva et al.2020] Fomicheva, Marina, Shuo Sun, Erick Fonseca, Frédéric Blain, Vishrav Chaudhary, Francisco Guzmán, Nina Lopatina, Lucia Specia, and André F. T. Martins. 2020. Mlqe-pe: A multilingual quality estimation and post-editing dataset.

[Garg et al.2019] Garg, Sarthak, Stephan Peitz, Udhyakumar Nallasamy, and Matthias Paulik. 2019. Jointly learning to align and translate with transformer models. In Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pages 4453–4462, Hong Kong, China, November. Association for Computational Linguistics.

[Müller et al.2020] Müller, Mathias, Annette Rios, and Rico Sennrich. 2020. Domain robustness in neural machine translation. In Proceedings of the 14th Conference of the Association for Machine Translation in the Americas (Volume I: Research Track), pages 151–164, Virtual, October. Association for Machine Translation in the Americas.

[Raunak et al.2021] Raunak, Vikas, Arul Menezes, and Marcin Junczys-Dowmunt. 2021. The curious case of hallucinations in neural machine translation. In Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pages 1172–1183, Online, June. Association for Computational Linguistics.

[Schulz et al.2020] Schulz, Karl, Leon Sixt, Federico Tombari, and Tim Landgraf. 2020. Restricting the flow: Information bottlenecks for attribution. In International Conference on Learning Representations.

[Sharou and Specia2022] Sharou, Khetam Al and Lucia Specia. 2022. A taxonomy and study of critical errors in machine translation. In Proceedings of the 23rd Annual Conference of the European Association for Machine Translation, pages 171–180, Ghent, Belgium, June. European Association for Machine Translation.

[Specia et al.2021] Specia, Lucia, Frédéric Blain, Marina Fomicheva, Chrysoula Zerva, Zhenhao Li, Vishrav Chaudhary, and André F. T. Martins. 2021. Findings of the WMT 2021 shared task on quality estimation. In Proceedings of the Sixth Conference on Machine Translation, pages 684–725, Online, November. Association for Computational Linguistics.

[Sundararajan et al.2017] Sundararajan, Mukund, Ankur Taly, and Qiqi Yan. 2017. Axiomatic attribution for deep networks. In Proceedings of the 34th International Conference on Machine Learning - Volume 70, ICML ’17, page 3319–3328. JMLR.org.

[Tu et al.2016] Tu, Zhaopeng, Zhengdong Lu, Yang Liu, Xiaohua Liu, and Hang Li. 2016. Modeling coverage for neural machine translation. In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), pages 76–85, Berlin, Germany, August. Association for Computational Linguistics.

[Vaswani et al.2017] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N
In July 1996, the journalist Ludmila Gorbul founded regular publication on Romanian language.

This is without prejudice to the Commission’s own administrative committee, which is composed of six local committees. The Commission shall be empowered to adopt delegated acts in accordance with Article 21 in order to adopt delegated acts in respect of:

six local councils have their own management committee.

The subsidies granted to the CCI-Airport and the CCI-Airport were granted on the basis of an agreement signed between the CCI and the CCI-Airport.

In the light of the above, the Commission concludes that the measures in question constitute State aid within the meaning of Article 107 (1) of the Treaty.

In this context, the Commission notes that there is a need for a number of measures to be taken in order to ensure that there is no undue negative impact on competition and trade.

In this context, the Commission notes that, in the light of the above, the Commission considers that it is appropriate to assess whether the measures at issue constitute State aid within the meaning of Article 107 (1) of the Treaty.

Figure 4: The fine-tuned model consistently outputs less hallucinations. In black: the source sentence. In red: the model output before fine-tuning (Transformer). In green: the baseline (cross-entropy with label-smoothed cross-entropy). In blue: our fine-tuned model.
The fine-tuned model consistently conveys the same translations on previously not hallucinated sentences. In black: the source sentence. In red: the model output before fine-tuning (Transformer). In green: the baseline (cross-entropy with label-smoothed cross-entropy). In blue: our fine-tuned model.
Gomez, Łukasz Kaiser, and Illia Polosukhin. 2017. Attention is all you need. In Advances in neural information processing systems, pages 5998–6008.

[Voita et al.2021] Voita, Elena, Rico Sennrich, and Ivan Titov. 2021. Analyzing the source and target contributions to predictions in neural machine translation. 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 1126–1140, Online, August. Association for Computational Linguistics.

[Welleck et al.2019] Welleck, Sean, Ilia Kulikov, Stephen Roller, Emily Dinan, Kyunghyun Cho, and Jason Weston. 2019. Neural text generation with unlikelihood training. CoRR, abs/1908.04319.