Towards Prediction Explainability through Sparse Communication

Marcos V. Treviso  
Instituto de Telecomunicações  
Lisboa, Portugal  
marcosvtreviso@gmail.com

André F. T. Martins  
Instituto de Telecomunicações & Unbabel  
Lisboa, Portugal  
andre.t.martins@tecnico.ulisboa.pt

Abstract

Explainability is a topic of growing importance in NLP. In this work, we provide a unified perspective of explainability as a communication problem between an explainer and a layperson about a classifier’s decision. We use this framework to compare several prior approaches for extracting explanations, including gradient methods, representation erasure, and attention mechanisms, in terms of their communication success. In addition, we reinterpret these methods at the light of classical feature selection, and we use this as inspiration to propose new embedded methods for explainability, through the use of selective, sparse attention. Experiments in text classification, natural language entailment, and machine translation, using different configurations of explainers and laypeople (including both machines and humans), reveal an advantage of attention-based explainers over gradient and erasure methods. Furthermore, human evaluation experiments show promising results with post-hoc explainers trained to optimize communication success and faithfulness.

1 Introduction

The widespread use of machine learning systems to assist humans in decision making brings the need for providing interpretations for models’ predictions (Lipton, 2018; Doshi-Velez and Kim, 2017; Rudin, 2019; Miller, 2019). This poses a challenge in NLP, where current state-of-the-art systems are based on deep neural networks and generally lack transparency (Goldberg, 2017; Peters et al., 2018; Devlin et al., 2019). Despite the large body of recent work in explainability (see §7 for a review), a unified perspective taking into account the human-machine interaction—a communication process in its essence—is still missing.

Many methods have been proposed to generate explanations. Some neural network architectures are equipped with built-in components—attention mechanisms—which weigh the relevance of input features for triggering a decision (Bahdanau et al., 2015; Vaswani et al., 2017). As a by-product, these weights provide plausible, but not always faithful, explanations (Jain and Wallace, 2019; Serrano and Smith, 2019; Wiegreffe and Pinter, 2019). Other approaches seek local explanations by evaluating the gradient of the predicted label with respect to the input features (Li et al., 2016a; Arras et al., 2017), or in a post-hoc manner by training a sparse linear model on a vicinity of the input example (Ribeiro et al., 2016) or by repeatedly querying the classifier with leave-one-out strategies (Li et al., 2016a; Feng et al., 2018).

How to assess the effectiveness of these different approaches? Several diagnostic tests have been proposed in prior work: Jain and Wallace (2019) assessed the explanatory power of attention weights by measuring their correlation with input gradients; Wiegreffe and Pinter (2019) and DeYoung et al. (2019) developed more informative tests, including a combination of comprehensiveness and sufficiency metrics and the correlation with human rationales. While useful, these frameworks rely on correlations and counterfactual simulation, and they do not provide a unified view of the existing
methods. They sidestep the main practical goal of prediction explainability—the ability to communicate an explanation to a human user.

In this work, we fill the gap above by proposing a unified framework that regards explainability as a communication problem: how can a machine communicate a justification for its decision (either a faithful explanation or a post-hoc interpretation) to a human? Our framework is inspired by human-grounded evaluation through forward simulation/prediction, as proposed by Doshi-Velez and Kim (2017, §3.2), where humans are presented with an explanation and an input, and must correctly simulate the model’s output (regardless of the true output). We simulate this process by considering the interaction between a classifier (the original model whose predictions we want to explain), an explainer (which provides the explanations), and a layperson (which must recover the classifier’s prediction). We experiment with explainers and laypeople being both humans and machines. Our framework allows comparing several prior approaches as different explainers, and inspires new ones: we propose explainers based on selective attention using sparsity (Martins and Astudillo, 2016; Peters et al., 2019), and a technique inspired by emergent communication (Foerster et al., 2016; Havrylov and Titov, 2017) that trains the explainer and layperson jointly.

Overall, our contributions are as follows:

- We draw a link between recent techniques for explainability of neural networks and classic feature selection in linear models (§2), leading to new embedded methods for explainability through selective, sparse attention (§3).

- We propose a new framework to assess explanatory power as the communication success rate between an explainer and a layperson (§4).

- We experiment with text classification, entailment, and machine translation, using different configurations of explainers and laypeople (humans or machines). This allows comparing in the same grounds models that use attention-based interpretations, post-hoc explanations, and gradient-based information (§5).

## 2 Static and Dynamic Feature Selection

A common way of generating explanations is by highlighting a small set of features (rationales, Zaidan and Eisner (2008)) that are considered relevant to the model’s decision (Lei et al., 2016; Ribeiro et al., 2016). A motivation for keeping this set small is the principle of parsimony (“Oc cam’s razor”), according to which simple explanations should be preferred over complex ones. The same principle has inspired a large body of work in sparse modeling and feature selection, although the connection between these two fields of research has been somewhat overlooked.

Traditional feature selection methods (Guyon and Elisseeff, 2003) are mostly concerned with model interpretability, where the goal is to understand how the model behaves globally. In this framework, feature selection happens statically during model training, and features that are deemed irrelevant are permanently deleted from the model. By contrast, most recent work in explaining neural networks address prediction explainability, where feature selection happens dynamically at runtime. Since explanations are input-dependent, features are never removed from the model (a feature that is not relevant for a particular input can be relevant for another).

Are these two worlds far away? Interestingly, the following typology, which originates from static feature selection (Guyon and Elisseeff, 2003, §4), still matches many existing approaches to dynamic feature selection (concrete examples in Table 1). The different methods are distinguished by the way they model the interaction between their main two components, the feature selector and the learning algorithm (in dynamic feature selection, these two components correspond to the explainer E and the classifier C, respectively). The typology consists of three classes of methods:

- **Wrapper methods**, in the wording of Guyon and Elisseeff (2003), “utilize the learning machine of interest as a black box to score subsets of variable according to their predictive power.” In static feature selection this means greedily searching over subsets of features, training a model with each candidate subset. In the dynamic feature selection world, this is somewhat reminiscent of the ablative analysis of Serrano and Smith (2019) or the leave-one-out method of Li et al. (2016b). Another example is LIME (Ribeiro et al., 2016), which involves repeatedly querying the classifier to label new examples. This class of methods requires multiple calls to the learning algorithm (in the case of static fea-
ture selection) or the classifier $C$ (in the case of dynamic feature selection).

- **Filter methods** decide to include/exclude a feature based on some importance metric (such as feature counts or pairwise mutual information). This can be done as a preprocessing step or by training the model once and thresholding the feature weights. In dynamic feature selection, this is done when we examine the gradient of the prediction with respect to each input feature, and then select the features whose gradient has large magnitude.\(^1\) This is the approach taken by the input gradient and layerwise relevance propagation techniques \cite{Li:2016:AIF, Arras:2016:RIP, Jain:2019:EAI}, where this gradient is taken as a measure of feature “importance.” Another example is when thresholding softmax attention scores to select relevant input features, as considered by \cite{Jain:2019:EAI} and \cite{Wiegrefe:2019:SAE} in their analyses. This class of methods involve at most one call to the classifier $C$.

- **Embedded methods**, in traditional feature selection, embed feature selection within the learning algorithm by using a sparse regularizer, such like the $\ell_1$-norm \cite{Tibshirani:1996:RFE}. Features that receive zero weight become irrelevant and can be removed from the model. In dynamic feature selection, this encompasses methods where the explainer $E$ is directly embedded in the classifier $C$, such as the method proposed by \cite{Lei:2016:3IF}. We propose in this paper \cite{§3} an alternative approach via sparse attention \cite{Martins:2016:SAA, Peters:2019:SIF}, where $C$ has a built-in mechanism, resembling $\ell_1$-regularization, that allows to select relevant input features and assign zero weight to everything else.

\(^1\)In linear models this gradient equals the feature’s weight.

In §4, we will frame each of the cases above as a component in a communication process, where the explainer $E$ aims to communicate a short message with the relevant features that triggered the classifier $C$’s decisions to a layperson $L$. The three cases above are distinguished by the way $C$ and $E$ interact.

## 3 Embedded Sparse Attention

The case where the explainer $E$ is embedded in the classifier $C$ naturally favors faithfulness, since the mechanism that explains the decision (the *why*) can also influence it (the *how*).

Attention mechanisms \cite{Bahdanau:2015:SSS} allow visualizing relevant input features that contributed to the model’s decision. Attention weights are usually computed by applying a softmax transformation to a vector of scores $s \in \mathbb{R}^n$, which are themselves a function of a query and key vectors. However, softmax-based attention is dense, i.e., it places some probability mass to every feature, even if small. The typical approach is to select the top-$k$ words with largest attention weights as the explanation. In the world of static feature selection, this is similar to what happens when using $\ell_2$-regularization for filtering: features whose weights have small magnitude are good candidates to remove from the model, i.e., their weights can be truncated to zero.

An alternative is to embed in the classifier an attention mechanism that is inherently selective, i.e., which can produce sparse attention distributions, where some input features receive exactly zero attention. Examples are the sparsemax \cite{Martins:2016:SAA} and the recently proposed 1.5-$\text{entmax}$ transformation \cite{Peters:2019:SIF}, described in detail in §A (supplemental material). These sparse attention transformations have been applied successfully in machine translation and morphological inflection applications \cite{Peters:2019:SIF}.

| Static selection (model interpretability) | Dynamic selection (prediction explainability) |
|------------------------------------------|-----------------------------------------------|
| **Wrappers**                              |                                                |
| Forward selection, backward elimination \cite{Kohavi:1997:AIF} | Input reduction \cite{Feng:2018:IPA}, representation erasure (leave-one-out) \cite{Li:2016:AIF, Serrano:2019:CRE} |
| **Filters**                               |                                                |
| Pointwise mutual information \cite{Church:1990:PIF}, recursive feature elimination \cite{Guyon:2002:RIF} | Input gradient \cite{Li:2016:AIF}, layerwise relevance propagation \cite{Bach:2015:LRP}, thresholding softmax attention |
| **Embedded**                              |                                                |
| $\ell_1$-regularization \cite{Tibshirani:1996:RFE}, elastic net \cite{Zou:2005:ENR} | Stochastic attention \cite{Xu:2015:SAE, Lei:2016:3IF}, sparse attention \cite{§3} |

Table 1: Overview of static and dynamic feature selection techniques.
We now have the necessary ingredients to describe emergent communication (Foerster et al., 2016; 4 Explainability as Communication
• proposed by Doshi-Velez and Kim (2017, evaluation through forward simulation/prediction, as framework is inspired by human-grounded eval-
either humans or machines. In the former case, our
In this paper, we experiment with E
cess of the communication is dictated by the ability
E
C
tions made by
E
m
is a message
E
C
Havrylov and Titov, 2017). Our starting point is the
4.1 The Classifier-Explainer-Layperson setup
Our framework draws inspiration on Lewis’ signal-
games (Lewis, 1969) and on the recent work on (emergent) communication (Foerster et al., 2016; Havrylov and Titov, 2017). Our starting point is the classifier
C : X → Y which, when given an input
x ∈ X, produces a prediction
y = C(x), and it has the possibility to access the internal representations
h exposed by
C. It outputs messages
m ∈ M that can be seen as a “rationale” for
y. The message
m = E(x, y, h) should be simple and compact enough to be easily transmitted and understood by the layperson
L. In this paper, we constrain the messages
m ∈ M to be bags-of-words (BoWs) extracted from the textual input
x, up to a maximum length of
k words.2
• The layperson
L is a simple model (e.g., a linear classifier) that receives the message
m as input, and predicts a final output
ŷ = L(m). The communication is successful if
y = ŷ. Given a test set
x₁, . . . , xₙ, we evaluate the communication success rate as the fraction of examples for which the communication was successful:

\[
\text{CSR} = \frac{1}{N} \sum_{n=1}^{N} \left[ \left[ C(x_n) = L(E(x_n, C(x_n))) \right] \right],
\]

(1)

where \([·]\) is the Iverson bracket notation.

Under this framework, we regard the communication success rate (CSR) as a quantifiable measure of explainability: a high CSR means that the layper-
son
L is able to replicate the classifier
C’s decisions a large fraction of the time when presented with the messages given by the explainer
E; this certifies that
E’s messages are informative enough.

4.2 Task examples
We show examples of how we can model the explainer and layperson for different NLP problems.

Text classification. We let
x ∈ X be a document (sequence of words), and the output space
Y a set of labels (e.g. topics or sentiment labels). If
C is an attention based classifier, then
E could just be a deterministic model that takes the attention probabilities from
C and truncates them to create a message
m as a small BoW.

Natural language entailment. Here, \(x\) is a pair of texts (a premise and an hypothesis) and the labels in
Y are entailment, contradiction, and neutral. We let messages be again BoWs, and we constrain them to be selected from the premise (and concatenate-
ated with the full hypothesis), as shown in Fig. 2.

Note that our framework is flexible about the choice of this message space
M. For example, explanations could also be prototypes, i.e., small subsets of training examples.
4.4 Joint training of explainer and layperson

Until now, we have assumed that the explainer $E$ is given beforehand, and that the layperson $L$ is a simple model that needs to be trained to assess the explanatory ability of $E$. But what if $E$ is also trained? For communication to succeed, $E$ and $L$ have to agree on a protocol that ensures informative messages. We will now see how $E$ and $L$ can be jointly trained, by learning to play a cooperative game (Lewis, 1969). Special care needs to be taken to ensure that the protocol they agree upon is not a “trivial” one: it has to retain information that is indeed useful to be regarded as a plausible, potentially faithful, explanation. We propose a strategy to ensure this, which will be validated using human evaluation in §6. We assume in this setting that explanations are extracted after $C$ is trained, i.e., $E$ is a post-hoc explainer.

A good explanation must be informative (both about the decision and the model’s decision process), compact, and understandable. The last two requirements are ensured by defining $M$ properly. But how to ensure the first requirement? To fully model the communication process and maximize the informativeness of the explanations $m$, we consider a strategy where both the explainer $E_\theta$ and layperson $L_\phi$ are trained models (with parameters $\theta$ and $\phi$), learned together to optimize a multi-task objective with two terms:

- A reconstruction term that controls the information about the classifier’s decision $\hat{y}$. We use a cross-entropy loss on the output of the layperson $L$, using $\hat{y}$ (and not the true label $y$) as the groundtruth: $\mathcal{L}(\phi, \theta) = -\log p_\phi(\hat{y} \mid m)$, where $m$ is the output of the explainer $E_\theta$.

- A faithfulness term that encourages the explainer $E$ to take into account, to some degree, the classifier’s decision process when producing its explanation $m$. To do this, we add a reconstruction loss term (using the cosine dissimilarity) that forces the explainer to predict also a continuous vector $h$ that should match the internal representation $\hat{h}$ that the classifier $C$ exposes: $\Omega(\theta) = 1 - \cos(\hat{h}(E_\theta), h)$.

The objective function to minimize is a combination of these two terms, $\mathcal{L}_\Omega(\phi, \theta) := \lambda \Omega(\theta) + \mathcal{L}(\phi, \theta)$, where $\lambda \geq 0$ is a constant tuned in a validation set. This function is minimized in a training set that contains pairs $(x, \hat{y})$. Therefore, in this
We used 4 datasets (SST, IMDB, AgNews, Yelp), we experimented with our framework in three NLP and for IWSLT to the source and target sentences.

Table 2: Dataset statistics. The average number of tokens for SNLI is related to the premise and hypothesis, and for IWSLT to the source and target sentences.

| Name  | # Train | # Test | Avg. tokens | # Classes |
|-------|---------|--------|-------------|-----------|
| SST   | 6920    | 1821   | 19          | 2         |
| IMDB  | 25K     | 25K    | 280         | 2         |
| AgNews| 115K    | 20K    | 38          | 2         |
| Yelp  | 5.6M    | 1M     | 130         | 5         |
| SNLI  | 549K    | 9824   | 14 / 8      | 3         |
| IWSLT | 206K    | 2271   | 20 / 18     | 134,086   |

Table 3 (columns 2–6) reports results for the communication success rate (CSR, Eq. 1) and for the accuracy of the layperson (ACC). By looking at the ACC column, we see a consistent drop from the RNN classifier to the layperson, regardless of the explainer. This is expected, since the layperson is a much weaker BoW classifier, and only has access to a limited number of words in the document. Note, however, that for some explainers (all the attention-based ones), this layperson outperforms a BoW classifier with access to all words. This is reassuring, as it shows that the layperson guided by the explainer outperforms an unguided layperson.

5 Experiments

We experimented with our framework in three NLP tasks (text classification, entailment, and machine translation), using the setup in §4.2.

5.1 Text classification

We used 4 datasets (SST, IMDB, AgNews, Yelp), with statistics in Table 2. We picked the same datasets as Jain and Wallace (2019) and Wiegrefe and Pinter (2019), excluding the smallest ones. For SST and IMDB we used the standard splits, and for AgNews and Yelp we randomly split the dataset, leaving 85% for training and 15% for test.

Classifier $C$. Each input word $x_i$ is mapped to 300D-pretrained GloVe embeddings (Pennington et al., 2014), kept frozen, followed by a 128D-bidirectional LSTM layer (BiLSTM), resulting in vectors $h_1, \ldots, h_n$. We score each of these vectors using the additive formulation from Bahdanau et al. (2015), applying an attention transformation to convert the resulting scores $s \in \mathbb{R}^n$ to a probability distribution $\pi \in \Delta^n$. We use this to compute a contextual vector $c = \sum_{i=1}^n \pi_i h_i$, which is fed into the output softmax layer that predicts $\hat{y}$. We trained our classifiers for at most 10 epochs, with a patience of 5 (for Yelp, we used 5 and 3, respectively), using AdamW (Loshchilov and Hutter, 2019), $\ell_2$ regularization with $\lambda = 0.01$, and default hyperparameters from PyTorch.

Layperson $L$ and explainer $E$. We used a simple linear BoW model as the layperson $L$. We evaluated three different types of explainers: (i) Erasure, a wrapper similar to the leave-one-out approaches of Jain and Wallace (2019) and Serrano and Smith (2019). We obtain the word with largest attention, “zero out” its input vector, and repass the whole input with the erased vector to the classifier $C$. We produce the message by repeating this procedure $k$ times and storing the erased words; (ii) Top-$k$ gradients, a filter approach that ranks word importance by their “input \times gradient” product, $|\frac{\partial y}{\partial x_i} \cdot x_i|$ (Ancona et al., 2018; Wiegrefe and Pinter, 2019). The top-$k$ words are selected as the message; (iii) Top-$k$ and selective attention: We experimented both using attention as a filter, by selecting the top-$k$ most attended words as the message, and embedded in the classifier $C$, by using the selective attentions described in §3 (1.5-entmax and sparsemax). We also report a random baseline, which randomly picks $k$ words as the message.

Regarding the CSR metric, the first thing to note is that, as expected, the random baseline does much worse than the other explainers, for all datasets. Among the non-trivial explainers, the erasure and top-$k$ attention explainers have similar performances in terms of CSR, with a slight advantage for attention methods. Note that the attention
We conducted experiments on the SNLI dataset (Table 2). We used a similar classifier \( C \) as the one in \( \S 5.1 \), except that now we have two inputs (the premise and the hypothesis). We used two independent BiLSTM layers, one for each. We used the additive attention of Bahdanau et al. (2015) with the last hidden state of the hypothesis as the query and the premise vectors as keys. The layperson differs from the one in \( \S 5.1 \) as follows: it uses a BiLSTM to encode the hypothesis, and then the BoWs from the explainer is passed through a linear projection and summed with the last hidden state of the BiLSTM, before the output layer.

The rightmost column of Table 3 shows a comparison for the explainers introduced in \( \S 5.1 \). The conclusion for SNLI is essentially the same as in text classification. The random baseline is very competitive, probably because just looking at the hypothesis is already a strong baseline (Gururangan et al., 2018). We also see that sparse attentions consistently perform better than other explainers. Moreover, when we truncate the attention distribution to top-\( k \) words the results are better then their fully embedded counterparts. We investigate the impact of the hyperparameter \( k \) in \( \S 5.4 \).

5.2 Natural language entailment

We conducted experiments on the SNLI dataset (Table 2). We used a similar classifier \( C \) as the one in \( \S 5.1 \), except that now we have two inputs (the premise and the hypothesis). We used two independent BiLSTM layers, one for each. We used the

| EXPLAINER | SST CSR | SST ACC | IMDB CSR | IMDB ACC | AGNEWS CSR | AGNEWS ACC | YELP CSR | YELP ACC | SNLI CSR | SNLI ACC |
|-----------|---------|---------|----------|---------|------------|------------|---------|---------|---------|---------|
| BoW       | 82.54   | 88.96   | 95.62    | 68.78   | 69.81      |            |         |         |         |         |
| RNN       | 86.16   | 91.79   | 96.28    | 75.80   |            | 78.34      |         |         |         |         |
| Random    | 69.41   | 70.07   | 67.30    | 66.67   | 58.27      | 53.06      | 75.83   | 68.74   |         |         |
| Erasure   | 80.12   | 81.22   | 92.17    | 88.72   | 78.72      | 69.90      | 77.88   | 70.04   |         |         |
| Top-k gradient | 79.35 | 79.24   | 95.09    | 94.86   | 70.54      | 62.86      | 76.74   | 69.40   |         |         |
| Top-k softmax | 84.18 | 82.43   | 93.06    | 89.46   | 81.00      | 70.18      | 78.66   | 71.00   |         |         |
| Top-k 1.5-entmax | 85.23 | 83.31   | 93.32    | 89.60   | 82.20      | 70.78      | 80.23   | 73.39   |         |         |
| Top-k sparsemax | 85.23 | 81.93   | 93.34    | 89.57   | 95.92      | 94.48      | 82.50   | 70.99   | 82.89   | 74.76   |
| Select. 1.5-entmax | 83.96 | 82.15   | 95.25    | 89.96   | 97.30      | 96.66      | 81.38   | 70.41   | 77.25   | 71.44   |
| Select. sparsemax | 85.23 | 81.93   | 93.24    | 89.66   | 95.92      | 94.48      | 83.55   | 71.60   | 82.04   | 73.46   |

Table 3: Results for text classification and SNLI datasets. CSR stands for the communication success rate, and ACC is the accuracy of the classifier/layperson. The top rows are the original classifiers, which access all words. The middle rows report performance for random, wrapper and filter explainers, for fixed \( k \)-word messages (the values of \( k \) for the several datasets are \{5, 10, 10, 10, 4\}, respectively). The bottom rows correspond to embedded methods where \( k \) is given automatically via sparsity. The average \( k \) obtained by 1.5-entmax and sparsemax are: SST: \{4.65, 2.59\}; IMDB: \{28.23, 12.94\}; AGNEWS \{5.65, 4.14\}; YELP: \{60.61, 23.86\}; SNLI: \{12.96, 8.27\}.
two vectors are concatenated and passed to a linear output layer to predict the next word $\tilde{y} \in \mathcal{Y}$ (see Fig. 3).

Results comparing different filtering methods varying $k$ are shown in Table 4. We show the CSR as we varied $k \in \{0, 1, 3, 5\}$. Again, top-$k$ attention performed better than top-$k$ gradient, in this case with a wider margin. In general, all methods perform better as we increase $k$, but we can already see a degradation of performance when $k = 5$ for all attention based explainers. An interesting case is when $k = 0$, meaning that $L$ has no access to the source sentence, behaving like an unconditioned language model. In this case the performance is much worse, indicating that both explainers are selecting relevant tokens when $k > 0$.

5.4 Trade-off between $k$ and CSR.

Figure 4 shows the trade-off between the length of the message and the communication success rate for different values of $k$ both for IMDB (text classification) and SNLI (natural language inference).

We see that as $k$ increases, CSR starts by increasing but then it starts dropping when $k$ becomes too large. This matches our intuition: in the two extreme cases where $k = 0$ and where $k$ is the document length (corresponding to a full bag-of-words classifier) the message has no information about how the classifier $C$ behaves. This behaviour is more clear for SNLI, where the average length of the premise is of 15 words only. By setting $k = 0$, meaning that the layperson $L$ only looks at the hypothesis, the CSR is reasonably high ($\sim 74\%$), but soon as we include a single word in the message this baseline is surpassed by 4 points or more. This is consistent with the previous finding that by considering only the hypothesis it is possible to achieve a high accuracy for SNLI (Gururangan et al., 2018).

6 Human Evaluation

Joint training of $E$ and $L$. So far we compared several given explainers, but what happens if we train $E$ and $L$ jointly to optimize CSR directly, as described in §4.4? We experiment with the IMDB and SNLI datasets, with $\lambda = 2$ for IMDB, $\lambda = 20$ for SNLI, and $\beta = 20\%$ for both. We contrast this with using humans for either the layperson, the explainer, or both.

Human layperson. We carried a portion of the explainers used in the previous experiments and we randomly selected 200 documents for IMDB and 100 for SNLI to be annotated by humans. The explanations (i.e. the selected words) were shuffled and displayed as a cloud of words to two annotators, who had to decide the label of each document. For SNLI, we show the entire hypothesis as raw text and the premise as a cloud of words. The annotation interface is shown in Fig. 5 (§A.3).

Human explainer. We also consider explanations generated by humans rather than machines. To this end, we used the e-SNLI corpus (Camburu et al., 2018), which extends the SNLI with human labeled marks on relevant words. Unfortunately, the e-SNLI corpus does not provide highlights over the premise for neutral pairs, and therefore we re-
Table 5: Results for human evaluation. \( H \)-CSR/ACC stands for human annotator (layperson) performance, \( L \)-CSR/ACC stand for machine layperson performance.

| EXPLAINER               | IMDB          | SNLI           |
|-------------------------|---------------|----------------|
|                         | \( H \)-CSR   | \( L \)-CSR   | \( H \)-ACC | \( L \)-ACC | \( H \)-CSR | \( L \)-CSR | \( H \)-ACC | \( L \)-ACC |
| Top-\( k \) gradient    | 73.75         | 84.50          | 70.75       | 80.50       | 66.00       | 76.00       | 78.50       | 75.00       |
| Top-\( k \) softmax     | 88.50         | 93.00          | 87.00       | 88.00       | 70.50       | 75.00       | 81.00       | 76.00       |
| Top-\( k \) 1.5-entmax  | 87.50         | 92.50          | 85.00       | 86.50       | \textbf{74.50} | 80.00       | 85.00       | 76.00       |
| Top-\( k \) sparsemax   | 90.00         | 89.50          | \textbf{89.50} | 88.00       | 73.00       | 86.00       | 81.50       | 76.00       |
| Joint \( E \) and \( L \)| \textbf{93.25} | \textbf{99.50} | 87.75       | \textbf{92.50} | 72.00       | \textbf{99.00} | 78.00       | \textbf{80.00} |
| Human highlights         | -             | -              | -           | -           | 69.00       | 76.00       | \textbf{86.50} | 77.00       |

moved the neutral class from the test set and obtained explanations using our trained models. We summarize our results in Table 5.

As in our previous experiments, better results were found both in terms of CSR and ACC for top-\( k \) attention methods in comparison to top-\( k \) gradient. Although we reported both \( H \)-CSR and \( L \)-CSR for the human highlights explainer, we point out that this explainer is not trained to match the classifier’s \( C \) decisions, which may explain the relatively low scores. The ACC of top-\( k \) attention models and human highlights explainers are close, reinforcing again the good results for attention-based models. Moreover, among the different attention explainers, we can see that sparsemax and 1.5-entmax outperform softmax in human scores.

As expected, the joint explainer achieves very high \( L \)-CSR, also outperforming all explainers in terms of \( L \)-ACC. The joint explainer was also able to achieve good human performance on IMDB, showing that it was able to optimize the communication and yet produce informative explanations. Whereas for SNLI, the human metrics are a bit lower in comparison with attention-based explainers, suggesting that in this case its explanations were not so informative. Outputs for these explainers can be consulted in §A.2.

7 Related Work

There is a body of recent work related to analysis and interpretation of neural networks. Our work is about prediction explainability, not to be confused with transparency or model interpretability—the difference between these concepts is made precise by Doshi-Velez and Kim (2017); Lipton (2018); Gilpin et al. (2018); Rudin (2019).

Recent works questioned the interpretative ability of attention mechanisms and whether they can be regarded as a form of explanation or not (Jain and Wallace, 2019; Serrano and Smith, 2019).

Wiegrefe and Pinter (2019) distinguished between faithful and plausible explanations and introduced several diagnostic tools to assess the usefulness of attention for explainability. None of these works, however, considers the sparse selective attention mechanisms we propose in this paper. Our goal is not to distinguish between faithful and plausible explanations. In contrast, we focus on better characterizing when explanations should be considered plausible, by providing a framework that gives an objective answer to this question. As discussed in Wiegrefe and Pinter (2019, §5), plausible explanations are very important even if not faithful: Rudin (2019) defines explainability as a plausible reconstruction of the decision-making process, and Riedl (2019) argues that they mimic what humans do when rationalizing past actions.

Gradient methods, such as DeepLIFT and Integrated Gradients (Bach et al., 2015; Montavon et al., 2018), leave-one-out strategies (Feng et al., 2018; Serrano and Smith, 2019), or post-hoc explainers such as LIME and Influence Functions (Ribeiro et al., 2016; Koh and Liang, 2017), have been proposed to generate or diagnose explanations, but the link between these approaches and filters and wrappers in the feature selection literature has not been made before. We believe the connections revealed in §2 will be potentially useful to develop new methods for model explainability.

Our framework draws inspiration from the field of emergent communication (Lazaridou et al., 2016; Foerster et al., 2016; Havrylov and Titov, 2017); some of the ideas proposed here (such as making the system end-to-end differentiable through sparsemax) may also be relevant in that field. The sparse, selective attention mechanisms that we propose in §3 are inspired by the “explanation selection” principle articulated by Miller (2019, §4): “Similar to causal connection, people do not typically provide all causes for an event
as an explanation. Instead, they select what they believe are the most relevant causes." Sparse and stochastic attention have been considered in several prior works (Xu et al., 2015; Lei et al., 2016; Martins and Astudillo, 2016; Peters et al., 2019; Bastings et al., 2019), but a systematic comparison with other attention and explanation strategies was still missing. Other approaches include Lei et al. (2016); Alvarez-Melis and Jaakkola (2017); Bastings et al. (2019).

Our work is also related to literature on sparse auto-encoders, which seek sparse overcomplete vector representations to improve model interpretability (Faruqui et al., 2015; Trifonov et al., 2018; Subramanian et al., 2018). In contrast to these works, we consider the probability distribution induced by sparse attention mechanisms as a form of explanation. Mullenbach et al. (2018) also use human evaluation to show that attention mechanism identifies meaningful explanations, which is consistent with our findings in §6.

Concurrently to our work, DeYoung et al. (2019) recently proposed a toolkit to compare different explanatory methods, distinguishing between comprehensive and sufficient rationales. Our work focus on sufficient rationales, not necessarily comprehensive, following the selective explanation principle of Miller (2019) stated above. Yet, their approach is orthogonal to ours and we believe both can benefit from each other.

8 Conclusions

We proposed a unified framework that regards explainability as a communication problem between an explainer and a layperson about a classifier’s decision. In doing so, we organized existing approaches in a typology that makes a bridge between traditional feature selection and modern explanation techniques, and which motivates our newly proposed embedded methods based on selective attention. In our experiments in text classification, entailment, and machine translation, we observed that attention mechanisms tend to outperform gradient methods and representation erasure on communication success rate, using both machines and humans as the layperson.

References

David Alvarez-Melis and Tommi Jaakkola. 2017. A causal framework for explaining the predictions of black-box sequence-to-sequence models. In Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, pages 412–421.

Marco Ancona, Enea Ceolini, Cengiz Öztireli, and Markus Gross. 2018. Towards better understanding of gradient-based attribution methods for deep neural networks. In Proc. ICLR.

Leila Arras, Franziska Horn, Grégoire Montavon, Klaus-Robert Müller, and Wojciech Samek. 2016. Explaining predictions of non-linear classifiers in NLP. In Proc. RepL4NLP, pages 1–7.

Leila Arras, Grégoire Montavon, Klaus-Robert Müller, and Wojciech Samek. 2017. Explaining recurrent neural network predictions in sentiment analysis. In Proc. WASSA.

Sebastian Bach, Alexander Binder, Grégoire Montavon, Frederick Klauschen, Klaus-Robert Müller, and Wojciech Samek. 2015. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. PloS one, 10(7):130–140.

Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio. 2015. Neural machine translation by jointly learning to align and translate. In Proc. ICLR.

Joost Bastings, Wilker Aziz, and Ivan Titov. 2019. Interpretable neural predictions with differentiable binary variables. In Proc. ACL.

Oana-Maria Camburu, Tim Rocktäschel, Thomas Lukasiewicz, and Phil Blunsom. 2018. e-snli: Natural language inference with natural language explanations. In Proc. NeurIPS, pages 9539–9549.

Mauro Cettolo, Marcello Federico, Luisa Bentivogli, Niehues Jan, Stüker Sebastian, Sudoh Katsuho, Yoshino Koichiro, and Federmann Christian. 2017. Overview of the iwslt 2017 evaluation campaign. In Proc. IWSLT, pages 2–14.

Kenneth Ward Church and Patrick Hanks. 1990. Word association norms, mutual information, and lexicography. Computational linguistics, 16(1):22–29.

Gonçalo M Correia, Vlad Niculae, and André FT Martins. 2019. Adaptively sparse transformers. In Proc. EMNLP-IJCNLP, pages 2174–2184.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. Bert: Pre-training of deep bidirectional transformers for language understanding. In Proc. NAACL-HLT, pages 4171–4186.

Jay DeYoung, Sarthak Jain, Nazneen Fatema Rajani, Eric Lehman, Caiming Xiong, Richard Socher, and Byron C Wallace. 2019. Eraser: A benchmark to evaluate rationalized nlp models. arXiv preprint arXiv:1911.03429.

Finale Doshi-Velez and Been Kim. 2017. Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.
Sofia Serrano and Noah A Smith. 2019. Is attention interpretable? In Proc. ACL.

Anant Subramanian, Danish Pruthi, Harsh Jhamtani, Taylor Berg-Kirkpatrick, and Eduard Hovy. 2018. Spine: Sparse interpretable neural embeddings. In Thirty-Second AAAI Conference on Artificial Intelligence.

Robert Tibshirani. 1996. Regression shrinkage and selection via the lasso. Journal of the Royal Statistical Society, 58(1):267–288.

Valentin Trifonov, Octavian-Eugen Ganea, Anna Potapenko, and Thomas Hofmann. 2018. Learning and evaluating sparse interpretable sentence embeddings. In Proc. EMNLP Workshop BlackboxNLP.

Constantino Tsallis. 1988. Possible generalization of boltzmann-gibbs statistics. Journal of Statistical Physics.

Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. 2017. Attention is all you need. In Proc. NeurISP, pages 5998–6008.

Sarah Wiegreffe and Yuval Pinter. 2019. Attention is not not explanation. In Proc. EMNLP-IJCNLP.

Kelvin Xu, Jimmy Ba, Ryan Kiros, Kyunghyun Cho, Aaron Courville, Ruslan Salakhudinov, Rich Zemel, and Yoshua Bengio. 2015. Show, attend and tell: Neural image caption generation with visual attention. In Proc. ICLR, pages 2048–2057.

Omar F Zaidan and Jason Eisner. 2008. Modeling annotators: A generative approach to learning from annotator rationales. In Proc. EMNLP, pages 31–40.

Hui Zou and Trevor Hastie. 2005. Regularization and variable selection via the elastic net. Journal of the royal statistical society, 67(2):301–320.
A Supplemental Material

A.1 Sparse attention

A natural way to get a sparse attention distribution is by using the sparsmax transformation (Martins and Astudillo, 2016), which computes an Euclidean projection of the score vector onto the probability simplex \( \Delta^n := \{ p \in \mathbb{R}^n | p \geq 0, \mathbf{1}^\top p = 1 \} \), or, more generally, the \( \alpha \)-entmax transformation (Peters et al., 2019):

\[
\alpha\text{-entmax}(s) := \arg \max_{p \in \Delta^n} p^\top s + H_\alpha(p),
\]

where \( H_\alpha \) is a generalization of the Shannon and Gini entropies proposed by Tsallis (1988), parametrized by a scalar \( \alpha \geq 1 \):

\[
H_\alpha(p) := \begin{cases} \frac{1}{\alpha(\alpha-1)} \sum_j (p_j - p_j^\alpha), & \alpha \neq 1 \\ -\sum_j p_j \log p_j, & \alpha = 1 \end{cases}
\]

(3)

Setting \( \alpha = 1 \) recovers the softmax function, while for any value of \( \alpha > 1 \) this transformation can return a sparse probability vector. Letting \( \alpha = 2 \), we recover sparsmax. A popular choice is \( \alpha = 1.5 \), which has been successfully used in machine translation and morphological inflection applications (Peters et al., 2019).

A.2 Examples of explanations

Table 6 shows the output of erasure, gradient, attention and joint explainers for four examples of IMDB. In Table 7 we also include the human highlights explainer for four pairs of SNLI.

A.3 Annotation interface

Figure 5 shows a snapshot of the annotation interface used for the experiments described in §6.
### EXPLANATIONS

**Table 6: Examples of extracted explanations for IMDB.**

| EXPLAINER | EXPLANATIONS |
|-----------|--------------|
| **(positive)** **Fun movie! Great for the kids - they found it very entertaining. Somewhat predictable, but there are a few surprises. Great movie to watch if you're looking for something just to entertain (don't expect to be seeing a classic!)** |
| Erasure | Great Great entertaining! Fun |
| Top-\(k\) gradient | Great Great! movie it |
| Top-\(k\) softmax | Great Great movie entertaining! |
| Top-\(k\) 1.5-entmax | Great Great to! entertaining |
| Top-\(k\) sparsemax | Great Great entertaining! Fun |
| Joint \(E\) and \(L\) | very entertaining Great movie |

| **(negative)** **This sequel to Problem Child is just as bad as the first one. It still teaches kids that it's O.K. to be bad. It's impossible for me to recommend this movie to anyone.** |
| Erasure | bad recommend Problem bad impossible |
| Top-\(k\) gradient | recommend Problem this to impossible |
| Top-\(k\) softmax | bad recommend impossible bad Problem |
| Top-\(k\) 1.5-entmax | bad impossible to bad recommend |
| Top-\(k\) sparsemax | bad impossible recommend bad kids |
| Joint \(E\) and \(L\) | bad bad |

| **(positive)** **When “The Net” was first being advertised, the ads made it look ridiculous. Then, when I saw it, it was actually quite good. Angela Bennett (Sandra Bullock) spends her days working on the computer and has never gotten to know her neighbors. Then, through a series of events, her identity gets erased by a cabal of shadowy people, and she can’t prove that she exists. Some parts of the movie are a little bit far-fetched; you’d probably know which parts if you saw the movie. Still, it’s a good look into what the existence of the Internet may have wrought on unsuspecting people. I do recommend it.** |
| Erasure | good good recommend ridiculous Still |
| Top-\(k\) gradient | ridiculous. good it recommend |
| Top-\(k\) softmax | good good recommend ridiculous do |
| Top-\(k\) 1.5-entmax | good do good actually quite |
| Top-\(k\) sparsemax | good good Still quite recommend |
| Joint \(E\) and \(L\) | good good movie recommend movie |

| **(negative)** **The film itself is only a compilation of scenes which have no inherent meaning to someone living outside of Russia. I won’t deny that some of the images and techniques were quite revolutionary at the time (filmed 1928) but the problem with the film is that it has no interest to the intellectual or common man. We are merely watching an arranged form of pictures, ranging from a one arm man beating a horse, to a toothless soldier in the war. Everything in between is awkward, haphazard and quite unnecessary. It would have been possible to invent a forum which kept the viewer interested but this would not be it although the method of the director is quite brilliant. In all, one should view this if they are an art student, on hallucinogenic drugs, or a student of pre-Tarkovskian cinema.** |
| Erasure | unnecessary brilliant haphazard compilation Everything |
| Top-\(k\) gradient | brilliant only problem haphazard unnecessary |
| Top-\(k\) softmax | unnecessary brilliant Everything compilation but |
| Top-\(k\) 1.5-entmax | brilliant unnecessary no problem no |
| Top-\(k\) sparsemax | brilliant unnecessary haphazard Everything problem |
| Joint \(E\) and \(L\) | no no would have |
| EXPLAINER | EXPLANATIONS |
|-----------|--------------|
| **(entailment)** | **hypothesis:** There is a person outside. **premise:** An adventurous man navigates through the jungle with a long stick. |
| Erasure | navigates stick jungle man |
| Top-\(k\) gradient | the jungle navigates . |
| Top-\(k\) softmax | navigates jungle stick adventurous |
| Top-\(k\) 1.5-entmax | adventurous man the navigates |
| Top-\(k\) sparsemax | navigates adventurous man the |
| Joint \(E\) and \(L\) | . jungle navigates stick |
| Human highlights | navigates through the jungle |
| **(contradiction)** | **hypothesis:** A biker rides next to the ocean. **premise:** A biker wearing glass and a backpack rides near a fountain. |
| Erasure | fountain glass rides biker |
| Top-\(k\) gradient | fountain near backpack a |
| Top-\(k\) softmax | fountain glass rides biker |
| Top-\(k\) 1.5-entmax | fountain glass rides biker |
| Top-\(k\) sparsemax | fountain glass backpack wearing |
| Joint \(E\) and \(L\) | biker A fountain glass |
| Human highlights | a fountain |
| **(entailment)** | **hypothesis:** A clad in denim person works is working on a bridge outdoors. **premise:** A man wearing a denim jacket and jeans welds on a bridge above water while wearing his safety mask. |
| Erasure | bridge water safety welds |
| Top-\(k\) gradient | welds . water jeans |
| Top-\(k\) softmax | bridge water welds man |
| Top-\(k\) 1.5-entmax | bridge man welds on |
| Top-\(k\) sparsemax | bridge a jeans man |
| Joint \(E\) and \(L\) | bridge . safety water |
| Human highlights | denim jacket bridge |
| **(contradiction)** | **hypothesis:** The teenager is riding a horse in a steeplechase competition. **premise:** A teen is standing in a field and is in the upswing position after hitting a golf ball. |
| Erasure | golf ball field a |
| Top-\(k\) gradient | in golf hitting ball |
| Top-\(k\) softmax | golf ball field hitting |
| Top-\(k\) 1.5-entmax | ball field golf after |
| Top-\(k\) sparsemax | ball . after field |
| Joint \(E\) and \(L\) | A teen field ball |
| Human highlights | standing in a field hitting a golf ball |

Table 7: Examples of extracted explanations for SNLI.