BARLE: Background-Aware Representation Learning for Background Shift Out-of-Distribution Detection

Hanyu Duan,1 Yi Yang,1 Ahmed Abbasi,2,3 Kar Yan Tam1

1 Department of Information Systems, Business Statistics and Operations Management, HKUST
2 Human-centered Analytics Lab, University of Notre Dame
3 Department of IT, Analytics, and Operations, University of Notre Dame

hduanac@connect.ust.hk, {imyiyang,kytam}@ust.hk, aabbasi@nd.edu

Abstract

Machine learning models often suffer from a performance drop when they are applied to out-of-distribution (OOD) samples, i.e., those drawn far away from the training data distribution. Existing OOD detection work mostly focuses on identifying semantic-shift OOD samples, e.g., instances from unseen new classes. However, background-shift OOD detection, which identifies samples with domain or style-change, represents a more practical yet challenging task. In this paper, we propose Background-Aware Representation Learning (BARLE) for background-shift OOD detection in NLP. Specifically, we generate semantics-preserving background-shifted pseudo OOD samples from pretrained masked language models. We then contrast the in-distribution (ID) samples with their pseudo OOD counterparts. Unlike prior semantic-shift OOD detection work that often leverages an external text corpus, BARLE only uses ID data, which is more flexible and cost-efficient. In experiments across several text classification tasks, we demonstrate that BARLE is capable of improving background-shift OOD detection performance while maintaining ID classification accuracy. We further investigate the properties of the generated pseudo OOD samples, uncovering the working mechanism of BARLE.

1 Introduction

Most state-of-the-art NLP models are evaluated with the assumption that the training data and testing data is drawn from the same distribution. However, when models are deployed in real-world settings, this assumption can be easily violated, and current NLP models tend to suffer from drastic performance drops on out-of-distribution (OOD) data (Hein et al., 2019; Hendrycks and Gimpel, 2016; Nguyen et al., 2015). Identifying OOD samples and distinguishing them from in-distribution (ID) ones, known as OOD detection, plays an essential role in a wide range of NLP applications (Kamath et al., 2020; Kumar and Sarawagi, 2019; Mukherjee and Awadallah, 2020).

Existing OOD detection methods in NLP mostly focus on identifying semantic-shift OOD samples (e.g., samples from unseen classes) (Yilmaz and Toraman, 2020; Zhan et al., 2021; Shu et al., 2017). However, Arora et al. (2021) point out that it is rare to encounter semantic-shift OOD inputs in real-world settings. In practice, background-shift OODs may be more pervasive. These are samples that belong to the same task as the ID data, but with a shift on background features, such as changes in the domain or the style of the text (Ren et al., 2019). For instance, a topic classification model trained on news articles (ID) vs. tweet messages (OOD), or a sentiment classification model trained on movie reviews (ID) vs. product reviews (OOD). Background-shift OOD detection represents a more practical yet challenging task. For example, consumer-facing manufacturers are routinely interested in building sentiment classification models to understand consumer sentiment for product-related issues in online reviews. However, such reviews also contain non-product design/aspect related reviews (such as retailer shipping and customer service experiences). If the sentiment classification model is applied to this review dataset without identifying the background-shift OODs (i.e., non-product design/aspect related reviews), the model may result in a lower prediction performance and thus negatively affect the company’s decision on product-related issues. Other applications of background-shift OOD include psychometric NLP tasks such as inferring users’ trust, anxiety, and literacy across domains like health and finance (Ahmad et al., 2020; Abbasi et al., 2021).

In this work, we propose an efficient and effective approach for background-shift OOD detection. First, our approach does not require any external data. Prior OOD detection methods often rely on external text corpora to simulate the OOD sam...
amples and learn ID-specific representations (Chen and Yu, 2021; Hendrycks et al., 2018; Xu et al., 2021). However, it is difficult to decide which external data to use, and the choice of the external dataset is critical for successful OOD detection (Hendrycks et al., 2018). Moreover, incorporating prior knowledge in choosing OOD data for training may introduce inductive bias to the OOD detector (Arora et al., 2021). In our work, we utilize pretrained language models (e.g., DistilBERT (Sanh et al., 2019), BERT (Devlin et al., 2018)) and perform a masked language modeling heuristic to generate semantics-preserving background-shifted pseudo samples from the ID data. For instance, a sentiment classification ID example “a sane and breathtakingly creative film” might be mapped to a pseudo example “a massive and perfectly executed painting”, where the background features (film) are replaced but the positive semantics is preserved. By taking advantage of pretrained language models, we can obtain better quality pseudo OODs in a more principled manner.

Second, we design a background-aware contrastive loss to push the ID training samples apart from their pseudo OOD counterparts. Combined with another semantic contrastive loss, the learned representations are not only semantically distinguishable (which is important for the main task) but also encode rich ID background information (which is important for OOD detection). We then employ an existing OOD scoring mechanism (Hendrycks and Gimpel, 2016; Liu et al., 2020; Lee et al., 2018; Zhou et al., 2021) to map the learned background-aware representation to a scalar that indicates the OOD likelihood.

Our approach is named BARLE, short for Background-Aware Representation Learning for identifying background-shift OODs. In experiments across several text classification tasks, we show that BARLE achieves superior performance in identifying background-shift OOD samples while maintaining the ID task performance. This implies that BARLE can be used as a 2-in-1 model which not only delivers desirable performance for the ID task, it can also detect any suspicious OOD samples. We also investigate the properties of generated pseudo OOD samples to better understand the working mechanism of BARLE, which may shed light on future OOD detection work. The code is publicly available via GitHub.  

1https://github.com/hduanac/BARLE. Our implementation is adapted from Zhou et al. (2021), we greatly appreciate the authors for releasing the code to the community.
language models (PLMs) to generate data for enhancing the performance of NLP tasks (Min et al., 2021), such as information extraction (IE) (Guo and Roth, 2021; Veyseh et al., 2021), sentiment analysis (SA) (Yu et al., 2021; Li et al., 2020), dataset generation (Schick and Schütze, 2021) and few shot learning (Schick and Schütze, 2020). To the best of our knowledge, no prior work has leveraged PLMs to augment ID samples and facilitate OOD detection, and our work demonstrates that this is a viable solution.

3 Method

3.1 Problem Formulation

We now formally define the background-shift OOD detection task. For a given dataset \( D_{ID} = \{(x_m, y_m)\}_{m=1}^M \) sampled from a data distribution \( P_{ID}(X, Y) \) (i.e., in-distribution), our goal is to build an OOD detector from \( D_{ID} \) to identify whether an arbitrary input \( x \) is drawn from the ID data distribution (i.e., \( P_{ID}(X, Y) \)) at inference time or not. We consider an input \((x, y)\) to be a background-shift OOD sample if \((x, y) \sim P_{OOD}(X, Y) \neq P_{ID}(X, Y)\), i.e., it is generated from a data distribution other than the ID data distribution \( P_{ID}(X, Y) \) but its class \( y \) belongs to one of the ID classes. We aim to learn an encoder \( \phi(x) : X \rightarrow \mathcal{H} \) that maps an instance \( x \) to a hidden representation \( h \in \mathcal{H} \). Then an OOD scoring mechanism further maps the hidden representation \( h \) to a scalar indicating the likelihood of the input \( x \) being OOD.

3.2 An Overview of BARLE

The overall framework of our proposed BARLE method is shown in Figure 1, and the procedure pseudocode is presented in Algorithm 1. It is composed of two major phases. In the first phase (§3.3), we generate pseudo OOD samples using ID training data by performing masked language modeling (MLM) with pretrained language models. This phase aims at synthesizing semantics-preserving background-shifted pseudo OOD samples. In the second phase (§3.4), we use contrastive learning on both the pseudo OOD samples and the ID training samples. We hope to learn background-aware and semantic-aware representations that can benefit not only the OOD detection but also the main task. Finally, given the learned representations, an OOD scoring mechanism is applied to identify the OOD likelihood.

Algorithm 1 Background-Aware Representation Learning (BARLE)

Input: ID training set \( D_{ID} \) and ID dev set \( D_{dev} \).
Output: Main task classifier with OOD detector.

/* Initialization step */
Load the generator \( G \) and main task model \( M \).

/* Pseudo OOD generation step */
for \( x \) in \( D_{ID} \)
do
  Generate \( \hat{x}^{pseudo} \) for \( x \) using \( G \).
  Add \( \hat{x}^{pseudo} \) to \( D_{pseudo} \).
end do

/* Contrastive representation learning step */
for \( t = 1, \ldots, T \)
do
  Sample from \( D_{ID} \) and \( D_{pseudo} \cup D_{ID} \).
  Calculate \( \mathcal{L}_{CE}, \mathcal{L}_{cons}, \) and \( \mathcal{L}_{conB} \).
  Total loss: \( L = \mathcal{L}_{CE} + \alpha \mathcal{L}_{cons} + \beta \mathcal{L}_{conB} \).
  Update the model parameters by \( L \).
end do
if \( t \% \text{stepsize} = = 0 \)
do
  Evaluate \( M \) with \( D_{dev} \).
end do
Return the best model.

3.3 Pseudo OOD Sample Generation

We leverage a pretrained masked language model to generate pseudo OOD samples using ID training data in a principled manner. To facilitate background-shift OOD detection, we expect to generate semantics-preserving background-shifted pseudo samples. Specifically, for a given instance \( x \) from the ID training set, we take a pretrained masked language model (such as BERT or DistilBERT), denoted as the generator \( G \), to produce a corresponding pseudo sample \( \hat{x}^{pseudo} \).

The generation process works as follows. The first step is to perform token masking. Given an instance \( x = [x_1, x_2, \ldots, x_n] \) as the input to the generator \( G \), say a sentence with \( n \) tokens, we randomly select one position \( m \) (an integer between 1 and \( n \)) to mask out. The token of the selected position \( m \) is replaced with a [MASK] token. We denote the masked instance as \( x^{masked} = REPLACE(x, m, [MASK]) \). The second step is to predict the masked token. The generator produces an output distribution over all the tokens in the vocabulary for that masked-out position, i.e., \( P_G(x_m \mid x^{masked}) \). We sample a token from this distribution (i.e., \( x_m \sim P_G(x_m \mid x^{masked}) \)) to replace the original token, i.e., \( \hat{x}^{pseudo} = REPLACE(x, m, x_m) \). Instead of sampling from the entire vocabulary, we sample the target token from a candidate set composed
of the tokens with top-$k$ highest probabilities because we want to avoid syntactic and semantic errors in the generated text. We apply the two steps iteratively until the replacement ratio $\rho$, the percentage of replaced tokens, achieves a pre-defined threshold. Finally, we add both the ID examples and the corresponding OOD samples together as $D_{ID} \cup D_{pseudo}$ for subsequent use.

We provide some examples of the generated pseudo OOD samples in Table 1. The examples provide us an intuitive understanding of the proposed pseudo OOD generation mechanism. We can observe that the background features such as movie and film of the ID data shift to diverse domain features such as painting and web, whereas the sentiment features are well-preserved in the generated pseudo OOD samples. Moreover, we also empirically show, in the experiment section, that the generated pseudo samples data can indeed preserve semantics but with background shift (See Figure 2).

### 3.4 Contrastive Representation Learning

We now present how to effectively utilize the pseudo OOD samples (§3.3) for background-shift OOD detection.

**Contrasting Background-Shifted Instances.** In prior works, most contrastive learning schemes applied to OOD detection problems act by pulling instances from the same semantic class closer while pushing samples with different class labels apart (Zeng et al., 2021a,b; Zhou et al., 2021). However, this may fail to detect background-shift OOD samples because such learning processes are mainly based on contrasting semantic features, while the background features are ignored. In other words, prior semantic-shift OOD detection works may very well distinguish a sentiment review from a restaurant review apart from a movie review.

To address this issue, we propose to contrast the ID training samples with their semantics-preserving background-shifted augmentations (i.e., the pseudo OOD samples) to encode the ID background information into the learned representations. We utilize a margin-based contrastive loss (Chopra et al., 2005). Specifically, we first sample a batch of instances $B = \{x_i\}_{i=1}^N$ from $D_{ID} \cup D_{pseudo}$, and let $x_i$ be a query instance drawn from the batch. If $x_i$ is an ID sample, all the ID samples in the batch except the query instance construct the positive set $\{x_i^+\}$, and the negative set $\{x_i^-\}$ is composed of all the pseudo OOD samples in the batch. Similarly, if $x_i$ is a pseudo OOD sample, the positive set consists of all the pseudo OOD samples in the batch except $x_i$, and all the ID samples in the batch construct the negative set. Formally, we denote the anchor set of the query instance $x_i$ as $A(x_i) = B \setminus x_i$. Then the positive set and the negative set are defined as $\{x_i^+\} = \{p \in A(x_i) : y_i = y_p\}$ and $\{x_i^-\} = \{n \in A(x_i) : y_i \neq y_n\}$, respectively. The background contrastive loss is formulated as:

$$\mathcal{L}_{pos}(x_i, \{x_i^+\}) = \sum_{x_i' \in \{x_i^+\}} \| \phi(x_i) - \phi(x_i') \|^2,$$

(1)

$$\mathcal{L}_{neg}(x_i, \{x_i^-\}) = \sum_{x_i' \in \{x_i^-\}} (\xi - \| \phi(x_i) - \phi(x_i') \|^2)_+,$$

(2)

$$\mathcal{L}_{conB} = \frac{1}{N} \left( \sum_{x \in B} \frac{1}{|\{x^+\}|} \mathcal{L}_{pos}(x, \{x^+\}) + \sum_{x \in B} \frac{1}{|\{x^-\}|} \mathcal{L}_{neg}(x, \{x^-\}) \right),$$

(3)

where the margin $\xi$ is defined following the prior work (Zhou et al., 2021) as the maximum distance between pairs of instances from the same class in a batch, and $\phi(x)$ denotes the hidden representation (i.e., the input to the softmax layer) of an instance.
Contrasting Semantically Different Instances.

We use another contrastive loss that contrasts semantically different instances. The idea is to learn compact semantic representation clusters, which may facilitate the main task performance. Similarly, we define the semantics contrastive loss as:

\[
    \mathcal{L}_\text{cons} = \frac{1}{N} \left( \sum_{x \in B_{1D}} \frac{1}{|\{x^+\}|} \mathcal{L}_{pos}(x, \{x^+\}) \right) \\
    + \sum_{x \in B_{1D}} \frac{1}{|\{x^-\}|} \mathcal{L}_{neg}(x, \{x^+\})), \tag{4}
\]

where \( B_{1D} \) denotes a batch of instances sampled from the ID training set \( D_{1D} \), and the positive set and negative set are constructed based on the class label of the main task. The model is also trained with cross-entropy loss \( \mathcal{L}_{CE} \). We formulate the overall total training loss as:

\[
    \mathcal{L} = \mathcal{L}_{CE} + \alpha \mathcal{L}_{cons} + \beta \mathcal{L}_{consB}. \tag{5}
\]

where \( \alpha \) and \( \beta \) control the strengths of the semantics contrasting and the background contrasting, respectively, both of which are tuned on the ID development set. With this loss, we expect the model to learn background-aware and task-specific representations that benefit not only the OOD detection but also the main task.

Finally, we use an OOD scoring mechanism to map the learned hidden representation to a scalar indicating the likelihood of the instance being an OOD sample. Various scoring mechanisms have been proposed such as MSP (Hendrycks and Gimpel, 2016), Energy (Liu et al., 2020), MHLNB (Lee et al., 2018) and Cosine (Zhou et al., 2021), and our proposed training scheme is scoring mechanism-agnostic. A brief introduction of these four scoring mechanisms and how they work with BARLE are presented in Appendix A.

### 4 Experiments

#### 4.1 Datasets

We consider two NLP tasks in the experiments: topic categorization and sentiment classification. For topic categorization, we use the Yahoo-AGNews-five testbed (Li et al., 2021). This dataset is composed of a subset of Yahoo!Answers as the ID data, and a subset of AGNews Corpus as the OOD data. The two datasets share the same label space, but their text style shifts.

For sentiment classification, we use three popular datasets (i.e., SST2, IMDB, and Amazon). Among the three datasets, SST2 and IMDB encompass movie reviews, whereas Amazon includes online consumer reviews of Amazon products (Blitzer et al., 2007). For the Amazon data, consistent with prior work, we retain the reviews from four categories (i.e., Books, DVDs, Electronics, and Kitchen appliances) to simulate the text domain shift scenario. The statistics of these datasets are shown in Table 2. These datasets have all been used in prior work for benchmarking semantic shift OOD detection (Hendrycks et al., 2020; Li et al., 2021).

<table>
<thead>
<tr>
<th>Dataset</th>
<th># ID training</th>
<th># ID dev</th>
<th># ID test</th>
<th># OOD test</th>
<th># Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo-AGNews-five</td>
<td>10,000</td>
<td>2,500</td>
<td>2,500</td>
<td>2,500</td>
<td>5</td>
</tr>
<tr>
<td>SST2</td>
<td>67,349</td>
<td>872</td>
<td>1,821</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>IMDB</td>
<td>22,500</td>
<td>2,500</td>
<td>25,000</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Amazon</td>
<td>6,400</td>
<td>800</td>
<td>800</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2: Statistics of the datasets.

We then construct the ID/OOD dataset pairs for background-shift OOD detection by pairing the datasets belonging to the same task, summarized in Table 3. We train the model on the ID training set, and the ID development set is used for param-
eter tuning. We evaluate the model's main task performance on the ID test set. The OOD detection performance is assessed on the OOD test set.

<table>
<thead>
<tr>
<th>Task</th>
<th>ID dataset</th>
<th>OOD dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic categorization</td>
<td>Yahoo!Answers</td>
<td>AGNews</td>
</tr>
<tr>
<td>Sentiment classification</td>
<td>Amazon</td>
<td>IMDM</td>
</tr>
<tr>
<td></td>
<td>Amazon</td>
<td>IMDM</td>
</tr>
<tr>
<td></td>
<td>Amazon-Books</td>
<td>Amazon-Electronics</td>
</tr>
<tr>
<td></td>
<td>Amazon-Kitchen</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: ID/OOD setups in the experiments.

### 4.2 Evaluation Metrics and Benchmarks

**Evaluation Metrics.** For OOD detection, we consider two commonly used metrics following prior work (Hendrycks and Gimpel, 2016; Lee et al., 2018), i.e., the AUROC and the FAR95. AUROC measures how much the model can distinguish the OOD samples from ID samples. Higher AUROC scores indicate better OOD detection capabilities, and a random guess detector would have an AUROC score of 0.5. FAR95 can be interpreted as the probability that an OOD sample (negative) is misclassified by the detector as an ID sample (positive) when the true positive rate (TPR) is equal to 95%. A lower FAR95 value indicates better OOD detection performance. We use classification accuracy (ACC) as the main task metric.

**Benchmarks.** Prior work has empirically showed that existing approaches for semantic-shift OOD detection perform poorly on background-shift OOD detection tasks, and there is little work on background-shift OOD detection (Arora et al., 2021; Li et al., 2021). Therefore, to choose suitable benchmarks to compare with, we consider the following two approaches. We first consider training the ID model using the vanilla cross-entropy loss on the ID data, only. We denote this benchmark as “Vanilla” (VAN). The second benchmark follows existing semantic shift OOD detection work by using an arbitrarily chosen external dataset as the pseudo OODs. We denote this benchmark as “External” (EXT). Following (Zhou et al., 2021), we choose the English text of a machine translation dataset (i.e., English-German WMT16 (Bojar et al., 2016)) as the auxiliary external data for EXT. In addition, we consider a density-based method (PPL) following (Arora et al., 2021). Specifically, we fine-tune GPT-2 (Radford et al., 2019) on the original ID data, and use the token perplexity as the OOD score. We implement the officially pretrained GPT-2 Small using the transformers library. 

### 4.3 Hyperparameter Settings

For pseudo OOD generation, we use the replacement ratio in the range of \{0.1, 0.3, 0.5, 0.7, 0.9\} and set the candidate size to 100. We do not substitute stopwords and synthesize pseudo OOD samples for all the ID training instances. For the representation learning, we build the classifier upon the officially pretrained RoBERTa (Liu et al., 2019) and BERT (Devlin et al., 2018) with different model scales using the transformers library. The model is optimized by AdamW (Loshchilov and Hutter, 2017) with 0.01 weight decay and 0.06 warmup ratio. We choose the learning rate from the range of \{1e-7, 1e-6\}, and we use a batch size of 8. The maximum sequence length is set to 256, and the parameters are tuned based on the contrastive loss and the classification performance on the ID development set.

To make it easier for practitioners to integrate BARLE in their working pipelines, we provide a guidance on hyperparameter selection as follows. For the replacement ratio \( \rho \), we recommend adjusting it based on the average length of input text. In general, we recommend setting a larger ratio (e.g., 0.5) for longer input text (e.g., hundreds of words on average) and smaller ratio (e.g., 0.1) for those with only dozens of words. For the number of generated pseudo OOD samples, we generate one pseudo OOD for one ID training example. As noted (§6), selecting informative pseudo OODs for efficient OOD detection may constitute an interesting future direction. For the top candidate \( k \), as we demonstrate in Figure 3, values that are too large or too small will not generate favourable pseudo OOD examples for the subsequent detection. We recommend a moderate size of 100 as a sensible default value.

### 4.4 Background-Shift OOD Detection Results

We use DistilBERT (Sanh et al., 2019) as the generator to synthesize pseudo OOD samples \(^5\) using the nlpaug library (Ma, 2019). We tune and set the contrastive loss hyperparameter \( \alpha \) and \( \beta \) to

---

\(^5\)https://huggingface.co/gpt2

\(^4\)https://github.com/huggingface/transformers

\(^5\)We also use BERT (Devlin et al., 2018) as the generator and find that the results are consistent. Thus we use DistilBERT in the experiments for its small scale and the efficiency purpose.
1.5 and 2.0 in the experiments. We use four different OOD scoring mechanisms, including MSP (Hendrycks and Gimpel, 2016), Energy (Liu et al., 2020), MHLNB (Lee et al., 2018) and Cosine (Zhou et al., 2021). Details about the scoring mechanisms appear in Appendix A.

The main experimental results (with RoBERTa-Large as the underlying model) appear in Table 4, Table 5 and Table 6. Full results using other pretrained models (RoBERTa-Base and BERT-Large/Base) are presented in Appendix B. First, we see that BARLE significantly outperforms benchmarks VAN and EXT on OOD detection, and the performance lift is consistent across tasks and datasets. The improvement over EXT indicates that our pseudo OOD generation is more effective than an arbitrary external dataset. Second, we find that BARLE gets more significant gains when combined with the density-based scoring mechanisms (i.e., MHLNB, and Cosine) compared with the calibration-based ones (MSP and Energy). We interpret this as follows: both density-based methods and our proposed contrastive losses work on the same hidden representation space so that such scoring mechanisms can directly benefit from the contrastively learned representations. This is consistent with (Arora et al., 2021) that density estimation methods can better account for background information shifts. We also examine the model’s main task classification accuracy on the ID testbed. The results appearing in Appendix C show that BARLE maintains desirable main task performance.

### Table 4: Topic categorization OOD detection.

<table>
<thead>
<tr>
<th>ID dataset</th>
<th>Model</th>
<th>OOD metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AUROC ↑ F1%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>GPT-2</td>
<td>0.596 0.942</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MSP</td>
<td>0.696 0.864</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Energy</td>
<td>0.740 0.778</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MHLNB</td>
<td>0.888 0.436</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Cosine</td>
<td>0.796 0.630</td>
</tr>
<tr>
<td>Yahoo!Answers</td>
<td>GPT-2</td>
<td>0.596 0.942</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MSP</td>
<td>0.704 0.883</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Energy</td>
<td>0.775 0.722</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MHLNB</td>
<td>0.945 0.288</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Cosine</td>
<td>0.991 0.495</td>
</tr>
<tr>
<td>SST2</td>
<td>GPT-2</td>
<td>0.596 0.942</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MSP</td>
<td>0.747 0.853</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Energy</td>
<td>0.788 0.764</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ MHLNB</td>
<td>0.960 0.210</td>
</tr>
<tr>
<td></td>
<td>RoBERTa-Large w/ Cosine</td>
<td>0.922 0.337</td>
</tr>
</tbody>
</table>

Table 5: Sentiment classification OOD detection.

### 4.5 Analysis of the Pseudo OOD samples

**Visualization of feature distributions.** Pseudo OOD sample generation using PLMs is a critical component in our work. Here, we compare the pseudo OOD feature distributions with that of the ID data. We use the SST2 dataset in this analysis. Following (Ren et al., 2019), we investigate the semantic feature and background feature distributions respectively. To capture the semantic features, we utilize the VADER lexicon⁶ to obtain sentiment scores of ID samples and pseudo OOD samples. We compare their sentiment polarity distributions in Figure 2 (left). We can observe that these two distributions are very well-overlapped, which indicates that the semantic meanings of the ID samples are well-preserved in the generated pair appear in Table 7. From the results, we can see that applying either the semantics-contrastive loss or the background-contrastive loss can outperform the one with the cross-entropy loss applied only. Moreover, applying the background-contrastive loss are more effective than applying the semantics-contrastive loss for background-shift OOD detection, and applying both can further improve the performance. The results on all eight ID/OOD pairs are presented in Appendix D.

---

⁶[https://www.nltk.org/api/nltk.sentiment.vader.html](https://www.nltk.org/api/nltk.sentiment.vader.html)
pseudo OOD samples. To examine the background features, we first train a doc2vec (Le and Mikolov, 2014) model with the ID training samples for capturing the surface ID background information. For each ID test sample and each pseudo OOD sample, we retrieve their most similar instances in the ID training set and calculate their cosine similarity scores. We plot the similarity score distributions in Figure 2 (right). We can see a clear distributional shift, which reflects the differences of the background statistics between the ID data and the generated pseudo OOD data. This analysis validates that BARLE can generate semantics-preserving background-shifted pseudo OOD samples.

**Hard Examples.** The quality of pseudo OOD samples is a common concern for OOD detection in prior works, as they often use external text corpus as OODs. In this analysis, we show that our generated pseudo OOD samples are “hard” negative examples whose native representations are located near the ID distribution. This is important because Robinson et al., 2020 show that contrastive learning can benefit from “hard” negative examples. Specifically, we fit a multivariate Gaussian distribution on the ID training (i.e., Amazon) examples’ hidden representations. We then measure the distance between the estimated distribution and each instance from the ID test set, the pseudo OOD set, and an arbitrarily chosen external set (i.e., WMT16) using the Mahalanobis distance metric. We visualize the distance distributions on a log scale in Figure 4. It shows that the pseudo OOD samples generated by BARLE are distributed much more closely to the ID samples on the hidden representation space compared with the arbitrarily chosen external instances, which shows that our generated pseudo OOD samples are hard examples. On the contrary, the external data distributions are far away from the ID test, indicating that they are easy negative examples so that contrastive learning may not sufficiently learn ID-specific information. This analysis also reveals that the common strategy of using external text corpora for background-shift OOD detection may not be effective.

**Sensitivity Analysis.** As part of our sensitivity analysis on pseudo OOD sample generation, we
Figure 3: Average OOD detection performances evaluated under different number of pseudo OOD samples (left), candidate sizes (mid), and replacement ratios (right). The candidate size "All" represents the entire vocabulary.

Figure 4: Distance distributions between ID training (Amazon data) and ID test, Pseudo OODs (our approach), and an external dataset respectively.

study the impact of 1). the number of pseudo OOD samples, 2). the candidate size $k$, and 3). the replacement ratio $\rho$ on the OOD detection performance. The analysis is conducted on the Yahoo-AGNews-five dataset and the results appear in Figure 3. Note that the AUROC score is averaged across the four scoring mechanisms. First, the OOD detection can benefit from a large number of pseudo OOD samples. In the main experiments, we generate one OOD sample for each of the ID samples, which corresponds to 10,000 OOD samples for this task. By decreasing the total number of pseudo OOD samples, we can see that the OOD detection performance decreases (Figure 3 (left)). Second, candidate size $k$ denotes the number of top-$k$ highest probability words to be considered for data augmentation. Figure 3 (mid) shows that neither large candidate size nor small candidate size produces optimal detection performance. This implies that we should adjust the candidate size according to the specific downstream tasks. Third, overly diversified pseudo OOD samples (i.e., large replacement ratio) cannot benefit OOD detection substantially (Figure 3 (right)). This is expected because the semantic features are likely to be changed in the pseudo OOD samples if the replacement ratio is large, and that would violate our objective of having semantics-preserving pseudo samples.

5 Conclusion

In this work, we propose a simple yet effective method for background shift OOD detection. Our method leverages pretrained language models to synthesize semantics-preserving background-shifted pseudo OOD samples from the ID training data. By contrasting the ID training samples with their pseudo OOD counterparts, our proposed training scheme learns background-aware representations and improves OOD detection performance. Additional analyses on the properties of the generated pseudo OOD samples also validates our design effectiveness. We believe our work sheds new light on OOD detection for building robust NLP systems. As noted, possible applications include an array of NLP-based user modeling tasks including inferring psychometrics, text-based personality detection in forums and social media (Yang et al., 2022), and stylometric authorship identification where style is the primary task and topics and genres are background (Abbasi and Chen, 2008).

6 Limitations

This work has several limitations that can be improved in future research. First, we do not evaluate the effectiveness of our proposed method on semantic-shift OOD detection, since our main focus is background-shift OOD detection. Future work can build upon our pseudo OOD generation approach and further investigate its performance on semantic-shift OOD detection, or develop a unified framework that can detect OODs of different kinds. Second, our approach generates one pseudo OOD for each of the ID training sample. This may not be very efficient for large datasets. Therefore, selecting informative pseudo OODs for efficient OOD
detection may constitute an interesting future direction. Third, our experiments are conducted on two text classification tasks where the label space is generally small (five for topic categorization and two for sentiment classification). How the approach performs in real-world NLP settings where the label space is large, or perhaps even going beyond text classification to prediction/regression tasks, warrants further investigation. Finally, our experiments show that the proposed approach works better with density-based OOD scoring mechanisms than with the calibration-based ones. This is consistent with (Arora et al., 2021) in that density-based methods can better account for background shifts. Future work may be needed to delve deeper into the relationship between OOD representation learning and OOD scoring mechanisms to better understand this OOD phenomenon.

Acknowledgements

We thank anonymous reviewers for their valuable comments and suggestions. This work was funded in part through U.S. NSF grant IIS-2039915 and an Oracle for Research grant entitled "NLP for the Greater Good."

References


Quoc Le and Tomas Mikolov. 2014. Distributed representations of sentences and documents. In International conference on machine learning, pages 1188–1196. PMLR.


A OOD Scoring Mechanisms

Our proposed method can generate background-aware representations. Given the representations, an OOD scoring mechanism is applied to infer the OOD likelihood. In this appendix, we briefly describe the OOD scoring mechanisms considered in our experiments.

**Maximum Softmax Probability (MSP).** MSP is first introduced for OOD detection by (Hendrycks and Gimpel, 2016). This method retrieves the maximum class probability from a softmax distribution for calculating the OOD score. Intuitively, higher maximum class probability implies lower likelihood of an OOD. Specifically, the MSP score is defined as:

\[
g_{\text{msp}} = 1 - \max_{i \in \{1, ..., C\}} p_i, \tag{6}\]

where \(C\) denotes the number of classes in a classification task, and \(p_i\) represents the softmax probability for the \(i\)-th class. The idea is that a more uniform softmax distribution indicates a higher likelihood to be OOD. Since our method BARLE is also trained with the main task, the output class probability can be directly used by MSP as the OOD likelihood.

**Energy Score (Energy).** Instead of using the maximum class probability, Liu et al., 2020 propose to measure an energy score of the output probabilities:

\[
g_{\text{energy}} = -\log \sum_{i=1}^{C} e^{w_i^T h}, \tag{7}\]

where \(w_i\) is the weight of the softmax layer in terms of the \(i\)-th class, and \(h\) denotes the input to the softmax layer, i.e., \(w_i^T h\) represents the logit corresponding to the \(i\)-th class label. The energy score can better distinguish ID and OOD samples since it is theoretically aligned with the probability density of the inputs, and less sensitive to the over-confidence issue. A higher energy score indicates a higher OOD likelihood. Similar to MSP, the output logits of BARLE are used to calculate the energy score.

**Mahalanobis Distance (MHLNB).** Lee et al., 2018 fit a class conditional Gaussian distribution on the ID development set \(\mathcal{D}_{\text{dev}} = \{(x_i, y_i)\}_{i=1}^{N}\) under Gaussian discriminant analysis. They first compute the empirical class mean and covariance by:

\[
\hat{\mu}_c = \frac{1}{N_c} \sum_{y_i = c} h_i, \tag{8}\]

\[
\hat{\Sigma} = \frac{1}{N} \sum_{c} \sum_{i, y_i = c} (h_i - \hat{\mu}_c)(h_i - \hat{\mu}_c)^T, \tag{9}\]

where \(c\) denotes the class label, \(N_c\) is the number of instances with the class \(c\), and \(h_i\) represents the input to the softmax layer of the \(i\)-th instance. Then, the detection score is defined by the Mahalanobis distance between the test sample and the closest class conditional Gaussian distribution, i.e.,

\[
g_{\text{MHLNB}} = \max_c - (h - \hat{\mu}_c)^T \hat{\Sigma}^{-1} (h - \hat{\mu}_c), \tag{10}\]

where \(h\) denotes the hidden representation (i.e., the input to the softmax layer) of the instance. The above metric corresponds to measuring the log of the probability density of the test sample in the estimated Gaussian distribution. The learned background-aware representations from BARLE can be utilized by MHLNB to infer its OOD likelihood.

**Cosine Similarity (Cosine).** We consider another distance metric based on the cosine similarity (Zhou et al., 2021). Given a test sample, the OOD score is defined by the maximum cosine similarity between the test sample and the instances in the development set:

\[
g_{\text{cosine}} = -\max_{i \in \{1, ..., N\}} \cos(h, h_i), \tag{11}\]

where \(N\) denotes the size of the development set, and \(h\) is the hidden representation, i.e., the input to the softmax layer. Similar to MHLNB, the learned representations from BARLE can be utilized by Cosine to infer its OOD likelihood.

B Additional OOD Detection Results

In the paper, we present the OOD detection results where the NLP tasks are fine tuned on RoBERTa-Large model. In this appendix, we change the underlying model to RoBERTa-Base, BERT-Base, and BERT-Large, and present the OOD results in Table 8 respectively.

C Main Task Performance

Although our focus is OOD detection, we need to examine if the background-aware representation learning will have negative effect on model’s main
Table 8: OOD detection performance of Yahoo-AGNews-five with different model scales.

Table 9: Main task classification performance averaged across four scoring mechanisms on RoBERTa-large.

D Full Ablation Study Results

We present the full ablation study results on all ID/OOD pairs in Table 11. The results consistently show that applying background-contrastive loss is more effective than semantics-contrastive loss in background-shift OOD detection, and applying both can further improve the performance.

Table 10: Main task classification performance averaged across four scoring mechanisms on Yahoo-AGNews-five with different model scales.
<table>
<thead>
<tr>
<th>Task</th>
<th>ID/OOD dataset pair</th>
<th>α/β</th>
<th>AUROC↑</th>
<th>FAR95↓</th>
<th>ACC↑</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic categorization</td>
<td>Yahoo!Answers / AGNews</td>
<td>-/-</td>
<td>0.780</td>
<td>0.677</td>
<td>0.829</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.792</td>
<td>0.636</td>
<td>0.822</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.843</td>
<td>0.553</td>
<td>0.842</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.854</td>
<td>0.543</td>
<td>0.830</td>
</tr>
<tr>
<td></td>
<td>Amazon-Books / Kitchen</td>
<td>-/-</td>
<td>0.695</td>
<td>0.922</td>
<td>0.954</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.719</td>
<td>0.903</td>
<td>0.950</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.732</td>
<td>0.931</td>
<td>0.953</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.739</td>
<td>0.927</td>
<td>0.950</td>
</tr>
<tr>
<td></td>
<td>Amazon-Books / Electronics</td>
<td>-/-</td>
<td>0.765</td>
<td>0.882</td>
<td>0.950</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.779</td>
<td>0.858</td>
<td>0.953</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.787</td>
<td>0.902</td>
<td>0.950</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.574</td>
<td>0.929</td>
<td>0.945</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.599</td>
<td>0.922</td>
<td>0.953</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.612</td>
<td>0.899</td>
<td>0.950</td>
</tr>
<tr>
<td></td>
<td>Amazon-Books / DVDs</td>
<td>-/-</td>
<td>0.587</td>
<td>0.459</td>
<td>0.960</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.899</td>
<td>0.438</td>
<td>0.956</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.927</td>
<td>0.424</td>
<td>0.947</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.949</td>
<td>0.380</td>
<td>0.954</td>
</tr>
<tr>
<td></td>
<td>SST2 / IMDB</td>
<td>-/-</td>
<td>0.880</td>
<td>0.574</td>
<td>0.956</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.890</td>
<td>0.464</td>
<td>0.946</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.908</td>
<td>0.428</td>
<td>0.946</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.908</td>
<td>0.428</td>
<td>0.946</td>
</tr>
<tr>
<td></td>
<td>SST2 / Amazon</td>
<td>-/-</td>
<td>0.641</td>
<td>0.918</td>
<td>0.949</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.621</td>
<td>0.933</td>
<td>0.958</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.687</td>
<td>0.831</td>
<td>0.951</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/+</td>
<td>0.925</td>
<td>0.599</td>
<td>0.955</td>
</tr>
<tr>
<td></td>
<td>Amazon / IMDB</td>
<td>-/-</td>
<td>0.965</td>
<td>0.243</td>
<td>0.949</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.977</td>
<td>0.106</td>
<td>0.958</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.981</td>
<td>0.083</td>
<td>0.953</td>
</tr>
<tr>
<td></td>
<td>Amazon / SST2</td>
<td>-/-</td>
<td>0.965</td>
<td>0.243</td>
<td>0.949</td>
</tr>
<tr>
<td></td>
<td></td>
<td>+/-</td>
<td>0.977</td>
<td>0.106</td>
<td>0.958</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/+</td>
<td>0.981</td>
<td>0.083</td>
<td>0.953</td>
</tr>
</tbody>
</table>

Table 11: Full results of applying different contrastive loss components on all eight ID/OOD pairs. The "-" and "+" denote setting the corresponding parameters to zeros or not respectively. The results are averaged across four scoring mechanisms.