Beyond Mahalanobis-Based Scores for Textual OOD Detection

Anonymous Author(s)
Affiliation
Address
email

Abstract

Deep learning methods have boosted the adoption of NLP systems in real-life applications. However, they turn out to be vulnerable to distribution shifts over time which may cause severe dysfunctions in production systems, urging practitioners to develop tools to detect out-of-distribution (OOD) samples through the lens of the neural network. In this paper, we introduce TRUSTED, a new OOD detector for Transformer architectures that meets operational requirements: it is unsupervised and fast to compute. The efficiency of TRUSTED relies on the fruitful idea that all hidden layers carry relevant information to detect OOD examples. Based on this, for a given input, TRUSTED consists in *(i)* aggregating this information and *(ii)* computing a similarity score by exploiting the training distribution, leveraging the powerful concept of *data depth*. Our extensive numerical experiments involve 51k model configurations, including various checkpoints, seeds, and datasets, and demonstrate that TRUSTED achieves state-of-the-art performances. In particular, it improves previous AUROC over 3 points.

1 Introduction

The number of AI systems put into production has steadily increased over the last few years. This is because advanced techniques of Machine Learning (ML) and Deep Learning (DL) have brought significant improvements over previous state-of-the-art (SOTA) methods in many areas such as finance [16, 43], transportation [45], and medicine [14, 61]. However, the increasing use of black-box models has raised concerns about their societal impact: privacy [22, 50], security [6, 3], safety [29, 37], fairness [5, 58], and explainability [13, 49] which became areas of active research in the ML community.

This paper is about a critical safety issue, namely Out-Of-Distribution (OOD) detection [11], which refers to a change of distribution of incoming data that may cause failures of in-production AI systems. When data are tabular and of small dimension, simple statistical methods can be efficient, and one may, for instance, monitor the mean and variance of each marginal over time. However, these traditional methods do not work anymore when data are high-dimensional and/or unstructured. Thus, the need to design new techniques that incorporate incoming data and the neural networks themselves.

Distinguishing OOD examples from in-distribution (ID) examples is challenging for modern deep neural architectures. DL models transform incoming data into latent representations from which reliable information extraction is cumbersome. Because of that, designing new tools of investigation for large pre-trained models, judiciously named *foundation* models by [9], is an essential line of research for the years to come. In computer vision, methods are more mature thanks to the availability of appropriate deformation techniques that allow for sensitivity analysis. In contrast, the nature

Submitted to 36th Conference on Neural Information Processing Systems (NeurIPS 2022). Do not distribute.

of tokens in Natural Language Processing (NLP) makes it more difficult to develop such suitable methods.

In this paper, we focus on textual data and on the ubiquitous `BERT` [23], `DistilBERT` [67], and `RoBERTa` [54] architectures. Existing methods can be grouped according to their positioning with respect to the network. Some works exploit only the incoming data and compare them with in-distribution examples through likelihood ratios [30, 17]. Another line of research consists in incorporating robust constraints during training, with [35] or without [82, 46] access to some available OOD examples. Another line of research focuses on post-processing methods that can be used on any pre-trained models. In our view, these are the most promising tools because typical users rely on transformers without retraining. Within post-processing methods, one can distinguish softmax-based tools that compute a confidence score based on the predicted probabilities and threshold to decide whether a sample is OOD or not. Notice that this does not require direct access to in-distribution data. The seminal work is due to Hendrycks [34] who uses the maximum soft-probability, and has been pushed further in [48, 39]. In [53], authors suggest looking one step deeper into the network, namely, to compute a confidence score based on the projections of the pre-softmax layer. More recently, [59] achieved SOTA results on transformer-based encoder by computing the Mahalanobis distance [57, 21] between a test sample and the in-distribution law [44], estimated through accessible training data points.

Nevertheless, the distance-based score is computed on the last-layer embedding only, suggesting that going deeper inside the network might improve OOD detection power. Moreover, the computation of Mahalanobis-based scores requires inverting the covariance matrix of the training data, which can be prohibitive in high dimensions. It is worth noticing that the Mahalanobis-based scores can be seen as a data depth [77, 83] through a simple re-scaling [52], that is a statistical function measuring the centrality of an observation with respect to a probability distribution. Although data depths are quite natural in the context of OOD detection, they remain overlooked by the ML community. In the present work, we rely on the recently introduced *Integrated Rank-Weighted depth* [60, 76] in order to remedy the drawbacks of the Mahalanobis-based scores for OOD detection.

1.1 Our contribution

We first leverage the observation introduced by previous work that *all* hidden layers of a neural network carry useful information to perform textual OOD detection. For a given input $\mathbf{x}$, our method consists in computing its average latent representation $\overline{\mathbf{x}}$ and then its OOD score through the depth score of $\overline{\mathbf{x}}$ with respect to the averaged in-distribution law (see Fig. 1 for an illustration). Notice that the ability to compute averaged latent representations crucially relies on the structure of transformers layers that share the same dimension. The depth function we are using is based on the computation of the projected ranks of the test inputs using randomly sampled directions. From a theoretical viewpoint, this novel method requires fewer assumptions on the data structure than the Mahalanobis score.

We conduct extensive numerical experiments on three transformers architectures and eight datasets and benchmark our method with previous approaches. To ensure reliable results, we introduce a new framework for evaluating OOD detection that considers hyperparameters that were unreported before. It consists of computing performances for various choices of checkpoints and seeds, which allows us to report a variance term that makes some previous methods fall within the same performance range. Our conclusions are drawn by considering over *51k configurations*, and show that our new detector based on data depth improves SOTA methods by 3 `AUROC` points while having less variance. This result supports the intuition that OOD detection is a matter of *looking at the information available across the entire network*. Our contribution can be summarized as follows:

1. **We introduce a novel OOD detection method for textual data.** Our detector `TRUSTED`[1] relies on the full information contained in pre-trained transformers and leverages the concept of data depth: a given input is detected as being in-distribution or OOD sample based on its depth score with respect to the training distribution.

2. **We conduct extensive numerical experiments** and prove that our method improves over SOTA methods. Our evaluation framework is more reliable than previous studies as it includes the variance with respect to seeds and checkpoints.

[1] `TRUSTED` stands for de**T**ecto**R** **US**ing in**T**egrated rank-w**E**ighted **D**epth.

3. **We release open-source code and data to ease future research**, ensure reproducibility and reduce computation overhead.

2 Problem Formulation

Training distribution and classifier. Let us denote by $\mathcal{X}$ the textual input space. Consider the multiclass classification setup with target space $\mathcal{Y} = \{1, \dots, C\}$ of size $C \geq 2$. We assume the dataset under consideration is made of $N \geq 1$ i.i.d. samples $(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_N, y_N)$ with probability law denoted by p_{XY} and defined on $\mathcal{X} \times \mathcal{Y}$. Accordingly, we will denote by p_X and p_Y the marginal laws of p_{XY}. Finally, we denote by $f_N : \mathcal{X} \to \mathcal{Y}$ the classifier that has been trained using $(\mathbf{x}_i, y_i)$.

Open world setting. In real-life scenarios, the trained model f_N is deployed into production and will certainly be faced with input data whose law is not p_{XY}. To each test point $(\mathbf{x}, y)$, we associate a variable $z \in \{0, 1\}$ such that $z = 0$ if $(\mathbf{x}, y)$ stems from p_{XY} and $z = 1$ otherwise. It is worth emphasizing that in our setting f_N has never been faced with OOD examples before deployment. This is usually referred to as the open-world setting. From a probabilistic viewpoint, the test set distribution of the input data p_X^{test} is a mixture of in-distribution and OOD samples:

$$p_X^{\text{test}}(\mathbf{x}) = \alpha \, p_{X|Z}(\mathbf{x}|z = 1) + (1 - \alpha) \, p_{X|Z}(\mathbf{x}|z = 0),$$

where $\alpha \in (0, 1)$. In this work, we will not make any further assumptions on the proportion α of OOD samples and on the OOD pdf $p_{X|Z}(\mathbf{x}|z = 1)$, making the problem more difficult but at the same time more well suited for practical use. Indeed, for textual data, it does not appear to be realistic to model how a corpus can evolve.

OOD detection. The objective of OOD detection is to construct a similarity function $s : \mathcal{X} \to \mathbb{R}_+$ that accounts for the similarity of any element in $\mathcal{X}$ with respect to the training in-distribution. For a given test input $\mathbf{x}$, we then classify $\mathbf{x}$ as in-distribution or OOD according to the magnitude of $s(\mathbf{x})$. Therefore, one fixes a threshold δ and classifies IN (*i.e.* $\hat{z} = 0$) if $s(\mathbf{x}) > \delta$ or OOD (*i.e.* $\hat{z} = 1$) if $s(\mathbf{x}) \leq \delta$. Formally, denoting $g(\cdot, \delta)$ the decision function, we take:

$$g(\mathbf{x}, \delta) = \begin{cases} 1 & \text{if } s(\mathbf{x}) \leq \delta, \\ 0 & \text{if } s(\mathbf{x}) > \delta. \end{cases} \tag{1}$$

Performance evaluation. The OOD problem is a (unbalanced) classification problem, and classically, two quantities allow to measure the performance of a method. The **false alarm rate** is the proportion of samples that are classified as OOD while they are IN. For a given threshold δ, it is theoretically given by $\Pr\big(s(\mathbf{X}) \leq \delta \,|\, Z = 0\big)$. The **true detection rate** is the proportion of samples that are predicted OOD while being OOD. For a given threshold δ, it is theoretically given by $\Pr\big(s(\mathbf{X}) \leq \delta \,|\, Z = 1\big)$.

There exist several ways to measure the effectiveness of an OOD method. We will focus on four metrics. The first two are specifically designed to assess the quality of the similarity function s.

Area Under the Receiver Operating Characteristic curve (`AUROC`) [10]. It is the area under the ROC curve $\delta \mapsto (\Pr\big(s(\mathbf{X}) > \delta \,|\, Z = 0\big), \Pr\big(s(\mathbf{X}) \leq \delta \,|\, Z = 1\big))$, which plots the true detection rates against the false alarm rates. The `AUROC` corresponds to the probability that an in-distribution example $\mathbf{X}_{in}$ has higher score than an OOD sample $\mathbf{X}_{out}$: $\texttt{AUROC} = \Pr(s(\mathbf{X}_{in}) > s(\mathbf{X}_{out}))$, as can be checked from elementary computations.

Area Under the Precision-Recall curve (`AUPR-IN`/`AUPR-OUT`) [20]. It is the area under the precision-recall curve $\delta \mapsto (\Pr\big(Z = 1 \,|\, s(\mathbf{X}) \leq \delta\big), \Pr\big(s(\mathbf{X}) \leq \delta \,|\, Z = 1\big))$ which plots the recall (true detection rate) against the precision (actual proportion of OOD amongst the predicted OOD). The `AUPR` is more relevant to unbalanced situations.

The third metric we will use is more operational as it computes the performance at a specific threshold δ corresponding to a security requirement.

False Positive Rate at 95% True Positive Rate (`FPR`). In practice, one wishes to achieve reasonable level of OOD detection. For a desired detection rate r, this incites to fix a threshold δ_r such that the corresponding TPR equals r. At this threshold, one then computes:

$$\Pr(s(\mathbf{X}) \geq \delta_r \,|\, z = 0) \quad \text{with} \;\; \delta_r \;\; \text{s.t.} \;\; \text{TPR}(\delta_r) = r. \tag{2}$$

In our work, we set $r = 0.95$ in (2).

Error of the best classifier (`Err (%)`). This refers to the lowest classification error obtained by choosing the best threshold.

3 TRUSTED: Textual OOD-Detection using Integrated Rank-Weighted Depth

In this work, we focus on OOD detection when using a contextual encoder (*e.g.*, BERT). We denote by $\{\phi_1, \dots, \phi_L\}$ the L functions corresponding to the layers of the encoder: for every $1 \leq l \leq L$ and a given textual input $\mathbf{x}$, $\phi_l(\mathbf{x}) \in \mathbb{R}^d$ is the embedding of $\mathbf{x}$ in the l-th layer, where d is the dimension of the corresponding embedding space. Notice that all layers share the same dimension d.

3.1 TRUSTED in a nutshell.

Our OOD detection method is composed of three steps. For a given input $\mathbf{x}$ with predicted label $\hat{y}$:

1. We first aggregate the latent representations of $\mathbf{x}$ via an aggregation function $F : \left(\mathbb{R}^d\right)^L \to \mathbb{R}^d$. We choose to take the mean and compute

$$F_{\mathrm{PM}}(\mathbf{x}) := F(\phi_1(\mathbf{x}), \dots, \phi_L(\mathbf{x})) = \frac{1}{L} \sum_{l=1}^{L} \phi_l(\mathbf{x}) := \overline{\mathbf{x}}.$$

We will further elaborate on this choice of aggregation function in Sec. 3.2.

2. We compute a similarity score $D(F_{\mathrm{PM}}(\mathbf{x}), F_{\mathrm{PM}}(\mathcal{S}^{\mathrm{train}}_{n,\hat{y}}))$ between $F_{\mathrm{PM}}(\mathbf{x})$ and the distribution of the mean-aggregation of the training distribution samples with same predicted target as $\mathbf{x}$ (*i.e.* $\hat{y}$) that we denote by $F_{\mathrm{PM}}(\mathcal{S}^{\mathrm{train}}_{n,\hat{y}})$. Formally, if $\mathbf{x}_1, \dots, \mathbf{x}_n$ are the training data, this distribution is given by $(1/n_{\hat{y}}) \sum_{i:\hat{y}_i=\hat{y}} \delta_{F_{\mathrm{PM}}(\mathbf{x}_i)}$, with $n_{\hat{y}} = |\{i : \hat{y}_i = \hat{y}\}|$. We take as similarity score D a depth function, namely the integrated rank-weighted depth, that we introduce in Sec. 3.3.

3. The last step consists in thresholding the previous similarity score $D(F_{\mathrm{PM}}(\mathbf{x}), F_{\mathrm{PM}}(\mathcal{S}^{\mathrm{train}}_{n,\hat{y}}))$: under a given threshold δ, we classify $\mathbf{x}$ as an OOD example.

3.2 Layer aggregation choice

Most recent work in textual OOD detection with a pre-trained transformer solely relies on the last layer of the encoder [80, 59]. Although detectors using information available in multiple layers have been proposed previously, mostly for image data, they rely on post-score aggregation heuristics that are either supervised [44, 31] (and thus require having access to OOD samples) or heavily use arbitrary heuristics [69]. TRUSTED differentiates from previous OOD detection methods as it relies on a pre-score aggregation function.

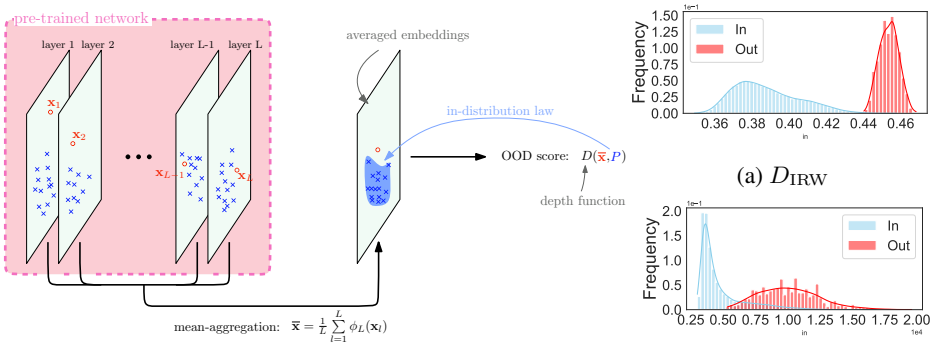
Most popular layer aggregation techniques for Transformer based architecture involve either Power Means [33, 66] or Wasserstein barycenters [18]. Motivated by both simplicity and computational efficiency, we discard the Wasserstein barycenters and decide to work with Power Mean (case $p = 1$).

3.3 OOD Score Computation via Integrated Rank-Weighted Depth

Since its introduction by John Tukey in 1975 [77] to extend the notion of median to the multivariate setting, the concept of statistical depth has become increasingly popular in multivariate data analysis. Multivariate data depths are nonparametric statistics that measure the centrality of any element of $\mathbb{R}^d$, where $d \geq 2$, w.r.t. a probability distribution (respectively a random variable) defined on any subset of $\mathbb{R}^d$. Let X be a random variable. We denote by P_X the law of X. Formally, a data depth is defined as follows:

$$\begin{array}{rccl} D: & \mathbb{R}^d \times \mathcal{P}(\mathbb{R}^d) & \longrightarrow & [0,1]\,, \\ & (\mathbf{x}, P_X) & \longmapsto & D(\mathbf{x}, P_X). \end{array} \tag{3}$$

The higher $D(\mathbf{x}, P_X)$, the deeper $\mathbf{x}$ is in P_X. Data depth finds many applications in statistics and ML ranging from anomaly detection [71, 64, 75] to regression [63, 32]. Numerous definitions have been proposed, such as, among others, the halfspace depth [77], the simplicial depth [51], the projection depth [52] or the zonoid depth [42], see [74, Ch. 2] for an excellent account of data depth. The halfspace depth is the most popular depth function probably due to its attractive theoretical properties



(a) D_{IRW}

(b) D_{M}

Fig. 1: TRUSTED detector. It relies on two steps: mean layer aggregation followed by the computation of D_{IRW}.

Fig. 3: Histogram scores.

[25, 83]. However, it is defined as the solution of an optimization problem (over the unit hypersphere) of a non-differentiable quantity and is therefore not easy to compute in practice [65, 27]. Recently, the Integrated Rank-Weighted (IRW) depth has been introduced in [60], replacing the infimum with an expectation (see also [15, 76]) in order to remedy this drawback. More precisely, the IRW depth of $\mathbf{x} \in \mathbb{R}^d$ w.r.t. to a probability distribution P_X on $\mathbb{R}^d$ is given by:

$$D_{\text{IRW}}(\mathbf{x}, P_X) = \int_{\mathbb{S}^{d-1}} \min \left\{ F_u\left(\langle \mathbf{u}, \mathbf{x} \rangle\right), 1 - F_u\left(\langle \mathbf{u}, \mathbf{x} \rangle\right) \right\} \mathrm{d}\mathbf{u},$$

where $F_u(t) = \Pr(\langle \mathbf{u}, \mathbf{X} \rangle \leq t)$ and $\mathbb{S}^{d-1}$ is the unit hypersphere. In practice, the expectation can be approximated by means of Monte-Carlo. Given a sample $\mathcal{S}_n = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$, the approximation of the IRW depth is defined as:

$$\widetilde{D}_{\text{IRW}}(\mathbf{x}, \mathcal{S}_n) = \frac{1}{n_{\text{proj}}} \sum_{k=1}^{n_{\text{proj}}} \min \left\{ \frac{1}{n} \sum_{i=1}^{n} \mathbb{I}\left\{ \langle \mathbf{u}_k, \mathbf{x}_i - \mathbf{x} \rangle \leq 0 \right\}, \frac{1}{n} \sum_{i=1}^{n} \mathbb{I}\left\{ \langle \mathbf{u}_k, \mathbf{x}_i - \mathbf{x} \rangle > 0 \right\} \right\},$$

where $\mathbf{u}_k \in \mathbb{S}^{d-1}$. The approximation version of the IRW depth can be computed in $\mathcal{O}(n_{\text{proj}} n d)$ and is then linear in all of its parameters. In addition, the IRW depth has many appealing properties such as invariance to scale/translation transformations or robustness [60, 15]. Furthermore, it has been successfully applied to anomaly detection [76] making it a natural choice for OOD detection.

Connection to Mahalanobis-based score. Interestingly enough, the Mahalanobis distance [57] can be seen as a data depth via an appropriate rescaling as suggested in [52]. It measures the distance between an element in $\mathbb{R}^d$ and a probability distribution having finite expectation and invertible covariance matrix differing from the Euclidean perspective by taking account of correlations. Precisely, the Mahalanobis depth function $D_{\text{M}}(\mathbf{x}, P_X)$ is defined as: $D_{\text{M}}(\mathbf{x}, p_X) = \left(1 + (\mathbf{x} - \mathbb{E}[\mathbf{X}])^\top \Sigma^{-1} (\mathbf{x} - \mathbb{E}[\mathbf{X}])\right)^{-1}$, where Σ^{-1} is the precision matrix of the r.v. $\mathbf{X}$. Even though interesting results relying on this notion have been highlighted in [59] for OOD detection, we experimentally observe better results with the IRW depth. Additionally, the Mahalanobis distance requires the first two moments to be finite and to compute Σ^{-1} in high dimension, which can be ill-conditioned in low data regimes. Last, inverting Σ requires $\mathcal{O}(d^3)$ operations or storing C matrix, which can become a burden when the number of classes grows [7].

Application to TRUSTED. The second step of TRUSTED uses an OOD score on the aggregated features. Thanks to its appealing properties, we choose to rely on the Integrated Rank-Weighted Depth D_{IRW} that measures the "similarity" between a test sample $\mathbf{x}$ and a training dataset $\mathcal{S}_n^{\text{train}}$. One independent D_{IRW} is computed per class on the final aggregated layer. The decision is taken by taking the D score of the predicted class. Formally the final score is taken as:

$$s_{\text{TRUSTED}}(\mathbf{x}) = D_{\text{IRW}}\left(F_{\text{PM}}(\mathbf{x}), F_{\text{PM}}\left(\mathcal{S}_{n,\hat{y}}^{\text{train}}\right)\right), \tag{4}$$

where we recall that $F_{\text{PM}}(\mathcal{S}_{n,\hat{y}}^{\text{train}})$ is the distribution of the mean-aggregation of the training distribution samples with same predicted target as $\mathbf{x}$ (*i.e.* $\hat{y}$).

4 Experimental Settings

In this section, we first discuss the limitation of the previous works on textual OOD detection, then present the chosen benchmark, the pre-trained encoders, and baseline methods.

4.1 Previous works and their limitations

Previous works in OOD detection [48, 68, 39, 53, 59] mostly rely on a single model to determine which methods are the best. This undermines the soundness of the conclusions that may only hold for the particular instance of the chosen model (*e.g.* for a specific checkpoint trained with a specific seed). To the best of our knowledge, no work studies the impact of the several sources of randomness that are involved, such as checkpoint and seed selections [70]). Nevertheless, these hyperparameters do impact the OOD detectors' performances. This is illustrated in Fig. 9 of the supplementary material, which gathers several Mahalanobis scores for various checkpoints of the same model.

In the light of Fig. 9, we choose to study both the impact of the checkpoint and the seed choice in our experiment. Specifically, for each model, we consider 5 different checkpoints. We save and probe models after 1k, 3k, 5k, 10k, 15k, and 20k finetuning steps. We additionally reproduce this experiment for 3 different seeds. As the reuse of checkpoints reduces the cost of research and allows for easy head-to-head comparison, our library also contains the probed models to draw general robust conclusions about the performance of the considered class of models [19, 26, 81].

4.2 Dataset selection

Dataset selection is instrumental for OOD detection evaluation as it is unreasonable to expect a detection method to achieve good results on any type of OOD data [1]. Since there is a lack of consensus on which benchmark to use for OOD detection in NLP, we choose to rely on the benchmark introduced by [82] which is an extension of the one proposed by [36].

Benchmark description. The considered benchmark is composed of three different types of in distribution datasets (referred to as `IN-DS`) which are used to train the classifiers: sentiment analysis (*i.e.*, SST2 [72] and IMDB [56]), topic classification (*i.e.*, 20Newsgroup [40]) and question answering (*i.e.*, TREC-10 [47]). For splitting we use either the standard split or the one provided by [82]. For the OOD datasets (referred to as `OUT-DS`), we first consider the aforementioned datasets (*i.e.*, any pair of datasets can be considered as OOD). Then, we also rely on four other datasets: a concatenation of premises and respective hypotheses from two NLI datasets (*i.e.*, RTE [12, 38] and MNLI [79]), Multi30K [28] and the source of the English-German WMT16 [8]. We gather in Tab. 5 the statistics of the various data-sets and refer the reader to reference [82] for further details.

4.3 Baseline methods and pre-trained models

Baseline methods. We consider the three following baselines[2]:

1. *Maximum Soft-max Probability* (MSP). This method has been proposed by [34]. Given an input $\mathbf{x}$, it relies on the final score s_{MSP} defined by $s_{\text{MSP}}(\mathbf{x}) = 1 - \max_{y \in \mathcal{Y}} p_{Y|X}(y|\mathbf{x})$, where $p_{Y|X}(\cdot|x))$ is the soft-probability predicted by the classifier after $\mathbf{x}$ has been observed.

2. *Energy-based score (E)* [53] is defined as the score $s_E(\mathbf{x}) = T \times \log \left[\sum_{y \in \mathcal{Y}} \exp\left(\frac{g_y(\mathbf{x})}{T}\right)\right]$, where $g_y(\mathbf{x})$ represents the logit corresponding to the class label y.

3. *Mahalanobis (D_{M})*. Following [59, 46, 82], the last layer of the encoder is considered leading to the score: $s_{\text{M}}(\mathbf{x}) = -D_{\text{M}}(F_{\text{PM}}(\mathbf{x}), F_{\text{PM}}(\mathcal{S}^{\text{train}}_{n,\hat{y}}))$ where $\hat{y}$ represents the label predicted by the classifier based on the observation of $\mathbf{x}$.[3]

Aggregation procedures. Both D_{M} and D_{IRW} rely on feature representations of the data which are extracted from the neural networks. For feature extraction we test four different strategies:

[2] Contrarily to [59], we do not use likelihood ratio as it would require using extra language models, which are not available in our setting.

[3] An alternative is to compute the minimum of all Mahalanobis distance computed on all the classes. However, we observe slightly better performance when using the predicted label $\hat{y}$.

1. *Logits layer selection*. We use the raw non-normalized predictions of the classifier. In this case $F_{Logits} \equiv F(\phi_1(\mathbf{x}), \ldots, \phi_L(\mathbf{x})) = \phi_{L+1}(\mathbf{x})$.

2. *Last layer selection*. Following previous work in textual OOD detection [80], we also consider the last layer of the network. Formally $F_L \equiv F(\phi_1(\mathbf{x}), \ldots, \phi_L(\mathbf{x})) = \phi_L(\mathbf{x})$.

3. *Layer concatenation*. We follow the `BERT` pooler and explore the concatenation of all layers. Formally, $F_{cat} \equiv F(\phi_1(\mathbf{x}), \ldots, \phi_L(\mathbf{x})) = [\phi_1(\mathbf{x}), \cdots, \phi_L(\mathbf{x})]$ represents the concatenated vector. The main limitation of layer concatenation is that the dimension of the considered features linearly increases with the number of layers which can be problematic for very deep networks [78].

Pretrained encoders. To provide an exhaustive comparison, we choose to work with different types of pre-trained encoders. We test the various methods on `DISTILBERT` (`DIS.`) [67], `BERT` [24] and `ROBERTA` (`ROB.`) [54]. We trained all models with a dropout rate [73] of 0.2, a batch size of 32, we use ADAMW [41]. Additionally, the weight decay is set to 0.01, the warmup ratio is set to 0.06 and the learning rate to 10^{-5}.

IN-DS	BERT Acc	DIS. Acc	ROB. Acc
20ng	92.9	92.0	92.7
imdb	91.7	90.6	93.6
sst2	92.7	91.7	95.2
trec	96.8	97.0	97.0

Tab. 1: Average test accuracy achieved by different classifier when training is initialized with different seeds.

5 Static Experimental Results

In this section, we demonstrate the effectiveness of our proposed detector using various pre-trained models. Due to space limitations, additional tables are reported in the Supplementary Material.

5.1 Methods comparison

Tab. 2: Average OOD detection performance (in %). The averages are taken over 1440 configurations and include four different `IN-DS` (20ng, imdb, sst2, trec), eight `OOD-DS`, three different seeds, five different checkpoints and three different pretrained encoders. Due to space constraints, different aggregations and related discussions are relegated to Appendix B.

Score	Aggregation	AUROC	AUPR-IN	AUPR-OUT	FPR	Err
E	F_{L+1}	89.9 $\pm$9.7	84.9 $\pm$19.0	79.9 $\pm$27.3	44.9 $\pm$33.4	23.9 $\pm$22.0
MSP	Soft.	89.7 $\pm$9.1	84.3 $\pm$18.9	80.4 $\pm$25.6	45.5 $\pm$29.5	25.4 $\pm$21.4
D_{M}	F_L	93.8 $\pm$9.8	89.2 $\pm$20.1	91.5 $\pm$16.4	19.8 $\pm$23.7	12.7 $\pm$17.0
	F_{L+1}	71.7 $\pm$13.7	54.7 $\pm$32.0	73.3 $\pm$28.4	62.6 $\pm$23.1	37.0 $\pm$22.9
	F_{cat}	90.4 $\pm$11.5	84.0 $\pm$22.1	88.0 $\pm$19.7	28.9 $\pm$26.2	17.6 $\pm$18.8
	F_{PM}	81.2 $\pm$15.3	67.7 $\pm$28.7	82.1 $\pm$22.2	40.2 $\pm$28.0	23.1 $\pm$20.3
D_{IRW}	F_L	92.6 $\pm$8.0	88.5 $\pm$17.7	86.3 $\pm$19.7	37.8 $\pm$27.3	23.6 $\pm$20.4
	F_{L+1}	82.4 $\pm$14.0	77.2 $\pm$24.0	72.1 $\pm$29.8	68.5 $\pm$29.5	38.0 $\pm$25.3
	F_{cat}	96.1 $\pm$4.9	91.8 $\pm$14.0	94.1 $\pm$11.4	19.1 $\pm$21.6	14.1 $\pm$16.2
TRUSTED	F_{PM}	**97.0** $\pm$**4.0**	**93.2** $\pm$**11.5**	**95.1** $\pm$**10.0**	**15.4** $\pm$**19.2**	**11.7** $\pm$**13.7**

In Tab. 2, we report the aggregated score obtained by each method combined with a different aggregation function. We observe that `TRUSTED` obtains the best overall scores followed by D_{IRW} using F_{cat}. Similarly to previous works [59], we notice in general that score leveraging information available from the training set (*i.e.*, D_{M} and D_{IRW}) achieve stronger results than those relying on output of softmax scores solely (*i.e.*, E and MSP).

Interestingly, we observe a large variation of performance of both D_{M} and D_{IRW}, *e.g.*, relying on the logits representations instead of using the last layer (*i.e.*, using F_{L+1} instead of F_L) hurts the performances of the methods. We observe a significant decrease in performance for D_{M} when averaging all the layers (case of F_{PM}), suggesting that the multivariate Gaussian assumption on which Mahalanobis approaches rely no longer hold for the resulting distribution.

5.2 On the pre-trained encoder choice

When training and deploying a classifier, a key question is choosing a pre-trained encoder. It can be beneficial in critical applications to trade off the main task accuracy to ensure better OOD detection. In Tab. 3, we report the individual performance of OOD methods on three types of classifiers.

Tab. 3: Average (over 480 model configurations) performance per pretrained encoder type.

Model	Score	Aggregation	AUROC	AUPR-IN	AUPR-OUT	FPR	Err
BERT	MSP	Soft.	89.6 ±9.3	84.1 ±19.8	80.8 ±25.5	46.4 ±30.8	25.8 ±22.4
	E	F_{L+1}	89.7 ±9.9	85.2 ±19.2	79.9 ±28.2	45.5 ±34.4	23.5 ±22.2
	D_{M}	F_L	95.9 ±6.9	91.9 ±17.3	93.1 ±15.4	15.9 ±21.5	10.7 ±15.1
		F_{L+1}	70.7 ±13.0	51.9 ±31.5	74.3 ±26.9	62.3 ±22.2	37.4 ±22.1
		F_{cat}	92.2 ±8.8	81.9 ±24.4	92.2 ±12.4	29.3 ±26.5	21.5 ±21.6
		F_{PM}	80.5 ±16.0	65.9 ±30.3	81.9 ±21.8	42.1 ±28.9	24.9 ±21.6
	D_{IRW}	F_L	92.6 ±7.7	88.7 ±18.2	87.0 ±19.1	38.0 ±27.8	23.8 ±20.4
		F_{L+1}	81.1 ±14.7	76.6 ±24.8	71.7 ±29.6	72.3 ±29.4	40.8 ±25.9
		F_{cat}	96.5 ±5.2	92.1 ±15.7	95.8 ±9.2	15.9 ±22.1	12.8 ±17.9
	TRUSTED	F_{PM}	**97.4** ±4.1	**93.6** ±12.8	**96.4** ±8.6	**12.6** ±19.6	**10.4** ±15.6
DIS.	MSP	Soft.	88.2 ±9.7	82.7 ±20.4	77.2 ±27.9	51.6 ±30.4	28.0 ±22.7
	E	F_{L+1}	88.1 ±10.9	83.3 ±20.8	77.1 ±29.4	50.3 ±36.1	26.2 ±24.1
	D_{M}	F_L	94.1 ±9.0	89.4 ±20.2	90.6 ±18.0	21.6 ±24.3	13.8 ±18.1
		F_{L+1}	72.3 ±13.9	55.7 ±33.1	72.3 ±29.3	63.8 ±23.1	37.8 ±24.0
		F_{cat}	89.2 ±11.6	83.9 ±21.7	85.6 ±21.5	30.8 ±25.7	17.4 ±18.2
		F_{PM}	80.0 ±15.6	68.6 ±28.4	79.2 ±24.7	43.8 ±28.1	24.1 ±20.8
	D_{IRW}	F_L	91.2 ±9.2	86.5 ±19.9	84.6 ±21.5	43.0 ±28.1	26.8 ±21.9
		F_{L+1}	78.4 ±15.4	73.5 ±25.5	67.8 ±32.1	76.1 ±26.3	41.7 ±25.9
		F_{cat}	96.3 ±3.9	91.5 ±13.3	94.0 ±11.7	18.9 ±20.7	14.3 ±14.9
	TRUSTED	F_{PM}	**97.3** ±2.9	**93.3** ±10.4	**95.1** ±9.9	**14.1** ±17.1	**11.1** ±11.5
ROB.	MSP	Soft.	91.4 ±7.9	85.9 ±16.4	83.0 ±23.0	39.1 ±26.0	22.6 ±18.7
	E	F_{L+1}	91.7 ±8.0	86.2 ±16.8	82.6 ±24.1	39.2 ±28.5	22.0 ±19.5
	D_{M}	F_L	91.7 ±11.9	86.6 ±22.0	90.9 ±15.5	21.6 ±24.7	13.5 ±17.5
		F_{L+1}	72.1 ±14.0	56.1 ±31.4	73.4 ±28.8	61.7 ±23.8	35.9 ±22.4
		F_{cat}	89.8 ±13.1	85.9 ±20.0	86.5 ±22.5	26.8 ±26.4	14.4 ±15.8
		F_{PM}	82.8 ±14.4	68.4 ±27.4	85.0 ±19.7	35.1 ±26.5	20.5 ±18.2
	D_{IRW}	F_L	93.8 ±6.6	90.2 ±14.7	87.4 ±18.2	32.9 ±25.3	20.5 ±18.4
		F_{L+1}	87.2 ±10.0	81.0 ±21.0	76.4 ±27.2	58.1 ±29.4	32.2 ±23.2
		F_{cat}	95.7 ±5.5	91.9 ±13.1	92.6 ±12.6	22.1 ±21.8	15.2 ±15.6
	TRUSTED	F_{PM}	**96.3** ±4.7	**92.7** ±11.3	**93.9** ±11.2	**19.1** ±20.2	**13.4** ±13.8

Although TRUSTED achieves state-of-the-art on all configurations, it is worth noticing a difference in performance concerning the type of pre-trained model. It is also important to remark that for ROB both MSP and E achieve on-par performances with D_{M} while not requiring any extra training information. Overall, for a given method (*i.e.* D_{M} or D_{IRW}), the ranking of detectors performances according to the type of feature extractor remain still. This validates the use of the mean-aggregation procedure of TRUSTED. Overall, based on the difference of OOD detection performance of Tab. 3, we recommend to use TRUSTED on BERT or DIS. if accurate OOD detection is required.

5.3 Impact of the training dataset

OOD detection performance depends on the nature of what is considered in-distribution (the training distribution in our case). Thus, it is interesting to study the performance per-IN-DS as reported in Tab. 4. Even though TRUSTED achieves strong results in terms of AUROC, we observe a high FPR on SST2. From Fig. 4, we observe that IMDB and SST2 are harder to detect, especially for D_{M}. Finally, since high AUROC does not necessarily imply a low FPR, it is crucial to take both into account when designing an OOD detector.

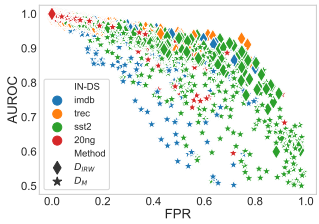


Fig. 4: AUROC&FPR trade-off.

IN-DS	Score	AUROC	AUPR-IN	AUPR-OUT	FPR	Err
20ng	TRUSTED	**98.4** ±1.8	**96.8** ±4.8	**98.0** ±4.2	**8.0** ±10.5	**6.4** ±6.8
	D_{M}	97.6 ±4.6	95.1 ±9.9	97.4 ±6.4	10.1 ±13.6	7.6 ±7.5
imdb	TRUSTED	**98.6** ±2.1	**99.8** ±0.4	**88.6** ±15.5	**8.0** ±13.9	**5.2** ±2.0
	D_{M}	93.3 ±9.8	98.0 ±5.4	77.3 ±24.7	19.3 ±20.6	6.4 ±2.8
sst2	TRUSTED	**93.8** ±5.8	**86.0** ±17.2	**93.9** ±9.4	**30.7** ±22.9	**22.1** ±17.9
	D_{M}	86.3 ±12.3	71.7 ±29.8	90.5 ±12.9	43.0 ±25.2	30.4 ±22.9
trec	TRUSTED	97.6 ±2.3	91.8 ±8.1	99.3 ±1.1	12.2 ±15.3	11.0 ±12.7
	D_{M}	**99.0** ±1.2	**94.9** ±6.8	**99.8** ±0.4	**4.4** ±7.4	**4.3** ±6.2

Tab. 4: Average OOD detection performance per IN-DS.

6 Dynamic Experimental Results

Most OOD detection methods are tested on specific checkpoints, where the selection criterion is often unclear. The consequences of this selection on OOD detection are rarely studied. This section aims to respond to this by measuring the OOD detection performance of methods on various checkpoint finetuning of the pre-trained encoder. We will use 5 different checkpoints taken after 1k, 3k, 5k, 10k, 15k, and 20k iterations. Training curves of the models are given in Fig. 7. Notice that after 3k iterations models have converged and no over-fitting is observed even after 20k iterations (*i.e.,* we do not observe an increase in validation loss).

Overall analysis. We report the results of the dynamic analysis on the various pre-trained models in Fig. 5. For all the methods and models (except D_{M} on `ROB`), we observe that training longer the classifier hurts detection. Interestingly, this drop in performance has a higher impact on `FPR` compared to `AUROC`. Thus, it *is better to use an early stopping criterion to ensure proper OOD detection performance.* In addition, we observed that `TRUSTED` (corresponding to D_{IRW}) achieves better detection results and that D_{M} outperforms `TRUSTED` for checkpoints larger than 10k on `ROB`.

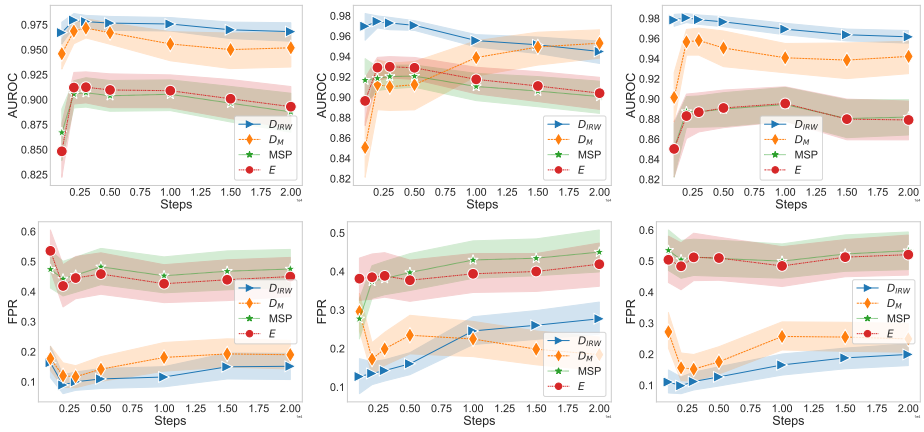


Fig. 5: Detection performance of different pretrained encoder during finetuning. First column correspond to `BERT`, second to `ROB` and last to `DIS`.

Analysis Per In-Dataset. Fig. 6 reports the results of the dynamical analysis per `IN-DS`. We observe that D_{IRW} is consistently better than D_{M} with sensible improvement on IMDB and SST2, which are the hardest benchmarks. We observe a similar trend to the previous experiment: *training longer the classifiers hurt their OOD detection performances*. Similar observations hold for `FPR`, `AUPR-IN`, and `AUPR-OUT` that are postponed to the Supplementary Material (see Fig. 10).

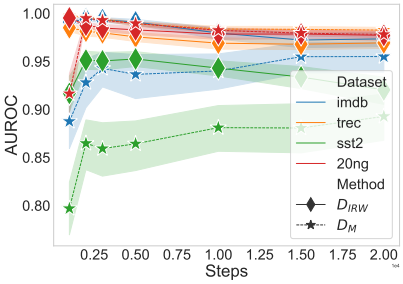


Fig. 6: `AUROC` per `IN-DS` during fine-tuning.

7 Conclusions and Future Directions

In this work, we introduced `TRUSTED` a novel OOD detector that relies on information available in all the hidden layers of a network. `TRUSTED` leverages a novel similarity score built on top of the Integrate Rank-Weighted depth. We conduct extensive numerical experiments proving that it consistently outperforms previous approaches, including detection based on the Mahalanobis distance. Our comprehensive evaluation framework demonstrates that, in general, OOD performances vary depending on several hyperparameters of the models, the datasets, and the detector's feature extraction step. Thus, we would like to promote the use of such exhaustive evaluation frameworks for future search to assess AI systems' safety tools properly. Another interesting question is the detection inference-time / accuracy trade-off, which is instrumental for the practitioner.

References

[1] Faruk Ahmed and Aaron Courville. Detecting semantic anomalies. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 3154–3162, 2020.

[2] Udit Arora, William Huang, and He He. Types of out-of-distribution texts and how to detect them. *arXiv preprint arXiv:2109.06827*, 2021.

[3] Ho Bae, Jaehee Jang, Dahuin Jung, Hyemi Jang, Heonseok Ha, Hyungyu Lee, and Sungroh Yoon. Security and privacy issues in deep learning. *arXiv preprint arXiv:1807.11655*, 2018.

[4] Anas Barakat and Pascal Bianchi. Convergence and dynamical behavior of the adam algorithm for non-convex stochastic optimization. *arXiv preprint arXiv:1810.02263*, 2018.

[5] Solon Barocas, Moritz Hardt, and Arvind Narayanan. Fairness in machine learning. *Nips tutorial*, 1:2, 2017.

[6] Marco Barreno, Blaine Nelson, Anthony D Joseph, and J Doug Tygar. The security of machine learning. *Machine Learning*, 81(2):121–148, 2010.

[7] K. Bhatia, K. Dahiya, H. Jain, P. Kar, A. Mittal, Y. Prabhu, and M. Varma. The extreme classification repository: Multi-label datasets and code, 2016. URL http://manikvarma.org/downloads/XC/XMLRepository.html.

[8] Ondrej Bojar, Rajen Chatterjee, Christian Federmann, Yvette Graham, Barry Haddow, Matthias Huck, Antonio Jimeno Yepes, Philipp Koehn, Varvara Logacheva, Christof Monz, Matteo Negri, Aurelie Neveol, Mariana Neves, Martin Popel, Matt Post, Raphael Rubino, Carolina Scarton, Lucia Specia, Marco Turchi, Karin Verspoor, and Marcos Zampieri. Findings of the 2016 conference on machine translation. In *Proceedings of the First Conference on Machine Translation*, pages 131–198, Berlin, Germany, August 2016. Association for Computational Linguistics. URL http://www.aclweb.org/anthology/W/W16/W16-2301.

[9] Rishi Bommasani, Drew A Hudson, Ehsan Adeli, Russ Altman, Simran Arora, Sydney von Arx, Michael S Bernstein, Jeannette Bohg, Antoine Bosselut, Emma Brunskill, et al. On the opportunities and risks of foundation models. *arXiv preprint arXiv:2108.07258*, 2021.

[10] Andrew P Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. *Pattern recognition*, 30(7):1145–1159, 1997.

[11] Saikiran Bulusu, Bhavya Kailkhura, Bo Li, Pramod K Varshney, and Dawn Song. Anomalous example detection in deep learning: A survey. *IEEE Access*, 8:132330–132347, 2020.

[12] J. Burger and L. Ferro. Generating an entailment corpus from news headlines. In *Proceedings of the ACL Workshop on Empirical Modeling of Semantic Equivalence and Entailment*, pages 49–54. Association for Computational Linguistics, 2005.

[13] Nadia Burkart and Marco F Huber. A survey on the explainability of supervised machine learning. *Journal of Artificial Intelligence Research*, 70:245–317, 2021.

[14] Ewen Callaway et al. Deepmind's ai predicts structures for a vast trove of proteins. *Nature*, 595 (7869):635–635, 2021.

[15] Bo Chen, Kai Ming Ting, Takashi Washio, and Gholamreza Haffari. Half-space mass: a maximally robust and efficient data depth method. *Machine Learning*, 100(2):677–699, 2015.

[16] Jiahao Chen, Victor Storchan, and Eren Kurshan. Beyond fairness metrics: Roadblocks and challenges for ethical ai in practice. *arXiv preprint arXiv:2108.06217*, 2021.

[17] Hyunsun Choi, Eric Jang, and Alexander A Alemi. Waic, but why? generative ensembles for robust anomaly detection. *arXiv preprint arXiv:1810.01392*, 2018.

[18] Pierre Colombo, Guillaume Staerman, Chloé Clavel, and Pablo Piantanida. Automatic text evaluation through the lens of Wasserstein barycenters. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 10450–10466, Online and Punta Cana, Dominican Republic, November 2021. Association for Computational Linguistics. doi: 10.18653/v1/2021.emnlp-main.817. URL https://aclanthology.org/2021.emnlp-main.817.

[19] Alexander D'Amour, Katherine Heller, Dan Moldovan, Ben Adlam, Babak Alipanahi, Alex Beutel, Christina Chen, Jonathan Deaton, Jacob Eisenstein, Matthew D Hoffman, et al. Underspecification presents challenges for credibility in modern machine learning. *arXiv preprint arXiv:2011.03395*, 2020.

[20] Jesse Davis and Mark Goadrich. The relationship between precision-recall and roc curves. In *Proceedings of the 23rd international conference on Machine learning*, pages 233–240, 2006.

[21] Roy De Maesschalck, Delphine Jouan-Rimbaud, and Désiré L Massart. The mahalanobis distance. *Chemometrics and intelligent laboratory systems*, 50(1):1–18, 2000.

[22] Yves-Alexandre de Montjoye, Ali Farzanehfar, Julien Hendrickx, and Luc Rocher. Solving artificial intelligence's privacy problem. *Field Actions Science Reports*, 17(1):80–83, 2017.

[23] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*, 2018.

[24] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, pages 4171–4186, Minneapolis, Minnesota, June 2019. Association for Computational Linguistics. doi: 10.18653/v1/N19-1423. URL https://aclanthology.org/N19-1423.

[25] David L. Donoho and Miriam Gasko. Breakdown properties of location estimates based on half space depth and projected outlyingness. *The Annals of Statistics*, 20:1803–1827, 1992.

[26] Rotem Dror, Segev Shlomov, and Roi Reichart. Deep dominance-how to properly compare deep neural models. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 2773–2785, 2019.

[27] Rainer Dyckerhoff and Pavlo Mozharovskyi. Exact computation of the halfspace depth. *Computational Statistics & Data Analysis*, 98:19–30, 2016.

[28] Desmond Elliott, Stella Frank, Khalil Sima'an, and Lucia Specia. Multi30K: Multilingual English-German image descriptions. In *Proceedings of the 5th Workshop on Vision and Language*, pages 70–74, Berlin, Germany, August 2016. Association for Computational Linguistics. doi: 10.18653/v1/W16-3210. URL https://aclanthology.org/W16-3210.

[29] José M Faria. Machine learning safety: An overview. In *Proceedings of the 26th Safety-Critical Systems Symposium, York, UK*, pages 6–8, 2018.

[30] Varun Gangal, Abhinav Arora, Arash Einolghozati, and Sonal Gupta. Likelihood ratios and generative classifiers for unsupervised out-of-domain detection in task oriented dialog. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 7764–7771, 2020.

[31] Eduardo Dadalto Camara Gomes, Florence Alberge, Pierre Duhamel, and Pablo Piantanida. Igeood: An information geometry approach to out-of-distribution detection. *arXiv preprint arXiv:2203.07798*, 2022.

[32] Marc Hallin, Davy Paindaveine, and Miroslav Šiman. Multivariate quantiles and multiple-output regression quantiles: From l1 optimization to halfspace depth. *The Annals of Statistics*, 38(2): 635–669, 04 2010.

[33] Godfrey Harold Hardy, John Edensor Littlewood, George Pólya, György Pólya, et al. *Inequalities*. Cambridge university press, 1952.

[34] Dan Hendrycks and Kevin Gimpel. A baseline for detecting misclassified and out-of-distribution examples in neural networks. *arXiv preprint arXiv:1610.02136*, 2016.

[35] Dan Hendrycks, Mantas Mazeika, and Thomas Dietterich. Deep anomaly detection with outlier exposure. *arXiv preprint arXiv:1812.04606*, 2018.

[36] Dan Hendrycks, Xiaoyuan Liu, Eric Wallace, Adam Dziedzic, Rishabh Krishnan, and Dawn Song. Pretrained transformers improve out-of-distribution robustness. *arXiv preprint arXiv:2004.06100*, 2020.

[37] Dan Hendrycks, Nicholas Carlini, John Schulman, and Jacob Steinhardt. Unsolved problems in ml safety. *arXiv preprint arXiv:2109.13916*, 2021.

[38] A. Hickl, J. Williams, J. Bensley, K. Roberts, B. Rink, and Y. Shi. Recognizing textual entailment with lcc's groundhog system. In *Proceedings of the Second PASCAL Challenges Workshop*, 2006.

[39] Yen-Chang Hsu, Yilin Shen, Hongxia Jin, and Zsolt Kira. Generalized odin: Detecting out-of-distribution image without learning from out-of-distribution data. *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 10948–10957, 2020.

[40] Thorsten Joachims. A probabilistic analysis of the rocchio algorithm with tfidf for text categorization. Technical report, Carnegie-mellon univ pittsburgh pa dept of computer science, 1996.

[41] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

[42] Gleb A. Koshevoy and Karl Mosler. Zonoid trimming for multivariate distributions. *The Annals of Statistics*, 25(5):1998–2017, 10 1997.

[43] Eren Kurshan, Hongda Shen, and Jiahao Chen. Towards self-regulating ai: Challenges and opportunities of ai model governance in financial services. In *Proceedings of the First ACM International Conference on AI in Finance*, pages 1–8, 2020.

[44] Kimin Lee, Kibok Lee, Honglak Lee, and Jinwoo Shin. A simple unified framework for detecting out-of-distribution samples and adversarial attacks. *Advances in neural information processing systems*, 31, 2018.

[45] Jesse Levinson, Jake Askeland, Jan Becker, Jennifer Dolson, David Held, Soeren Kammel, J Zico Kolter, Dirk Langer, Oliver Pink, Vaughan Pratt, et al. Towards fully autonomous driving: Systems and algorithms. In *2011 IEEE intelligent vehicles symposium (IV)*, pages 163–168. IEEE, 2011.

[46] Xiaoya Li, Jiwei Li, Xiaofei Sun, Chun Fan, Tianwei Zhang, Fei Wu, Yuxian Meng, and Jun Zhang. k folden: k-fold ensemble for out-of-distribution detection. *arXiv preprint arXiv:2108.12731*, 2021.

[47] Xin Li and Dan Roth. Learning question classifiers. In *COLING 2002: The 19th International Conference on Computational Linguistics*, 2002. URL https://aclanthology.org/C02-1150.

[48] Shiyu Liang, Yixuan Li, and R. Srikant. Enhancing the reliability of out-of-distribution image detection in neural networks. In *International Conference on Learning Representations*, 2018. URL https://openreview.net/forum?id=H1VGkIxRZ.

[49] Pantelis Linardatos, Vasilis Papastefanopoulos, and Sotiris Kotsiantis. Explainable ai: A review of machine learning interpretability methods. *Entropy*, 23(1):18, 2020.

[50] Bo Liu, Ming Ding, Sina Shaham, Wenny Rahayu, Farhad Farokhi, and Zihuai Lin. When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys (CSUR)*, 54 (2):1–36, 2021.

[51] Regina Y. Liu. On a notion of data depth based on random simplices. *The Annals of Statistics*, 18(1):405–414, 1990.

[52] Regina Y. Liu. *Data depth and multivariate rank tests*, pages 279–294. 1992.

[53] Weitang Liu, Xiaoyun Wang, John Owens, and Yixuan Li. Energy-based out-of-distribution detection. *Advances in Neural Information Processing Systems*, 2020.

[54] Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. Roberta: A robustly optimized bert pretraining approach. *arXiv preprint arXiv:1907.11692*, 2019.

[55] Ilya Loshchilov and Frank Hutter. Decoupled weight decay regularization. *arXiv preprint arXiv:1711.05101*, 2017.

[56] Andrew L. Maas, Raymond E. Daly, Peter T. Pham, Dan Huang, Andrew Y. Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, pages 142–150, Portland, Oregon, USA, June 2011. Association for Computational Linguistics. URL https://aclanthology.org/P11-1015.

[57] Prasanta Chandra Mahalanobis et al. On the generalised distance in statistics. In *Proceedings of the National Institute of Sciences of India*, volume 2, pages 49–55, 1936.

[58] Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan. A survey on bias and fairness in machine learning. *ACM Computing Surveys (CSUR)*, 54(6):1–35, 2021.

[59] Alexander Podolskiy, Dmitry Lipin, Andrey Bout, Ekaterina Artemova, and Irina Piontkovskaya. Revisiting mahalanobis distance for transformer-based out-of-domain detection. *arXiv preprint arXiv:2101.03778*, 2021.

[60] Kelly Ramsay, Stéphane Durocher, and Alexandre Leblanc. Integrated rank-weighted depth. *Journal of Multivariate Analysis*, 173:51–69, 2019.

[61] Bharath Ramsundar, Steven Kearnes, Patrick Riley, Dale Webster, David Konerding, and Vijay Pande. Massively multitask networks for drug discovery. *arXiv preprint arXiv:1502.02072*, 2015.

[62] Jie Ren, Peter J Liu, Emily Fertig, Jasper Snoek, Ryan Poplin, Mark A DePristo, Joshua V Dillon, and Balaji Lakshminarayanan. Likelihood ratios for out-of-distribution detection. *arXiv preprint arXiv:1906.02845*, 2019.

[63] Peter J. Rousseeuw and Mia Hubert. Regression depth. *Journal of the American Statistical Association*, 94(446):388–402, 1999.

[64] Peter J. Rousseeuw and Mia Hubert. Anomaly detection by robust statistics. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 8(2):e1236, 2018.

[65] Peter J. Rousseeuw and Anja Struyf. Computing location depth and regression depth in higher dimensions. *Statistics and Computing*, 8(3):193–203, 1998.

[66] Andreas Rücklé, Steffen Eger, Maxime Peyrard, and Iryna Gurevych. Concatenated power mean word embeddings as universal cross-lingual sentence representations. *arXiv preprint arXiv:1803.01400*, 2018.

[67] Victor Sanh, Lysandre Debut, Julien Chaumond, and Thomas Wolf. Distilbert, a distilled version of bert: smaller, faster, cheaper and lighter. *arXiv preprint arXiv:1910.01108*, 2019.

[68] Chandramouli Shama Sastry and Sageev Oore. Detecting out-of-distribution examples with Gram matrices. In Hal Daumé III and Aarti Singh, editors, *Proceedings of the 37th International Conference on Machine Learning*, volume 119 of *Proceedings of Machine Learning Research*, pages 8491–8501. PMLR, 13–18 Jul 2020. URL https://proceedings.mlr.press/v119/sastry20a.html.

[69] Chandramouli Shama Sastry and Sageev Oore. Detecting out-of-distribution examples with gram matrices. In *International Conference on Machine Learning*, pages 8491–8501. PMLR, 2020.

[70] Thibault Sellam, Steve Yadlowsky, Jason Wei, Naomi Saphra, Alexander D'Amour, Tal Linzen, Jasmijn Bastings, Iulia Turc, Jacob Eisenstein, Dipanjan Das, et al. The multiberts: Bert reproductions for robustness analysis. *arXiv preprint arXiv:2106.16163*, 2021.

[71] Robert Serfling. Depth functions in nonparametric multivariate inference. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 72, 2006.

[72] Richard Socher, Alex Perelygin, Jean Wu, Jason Chuang, Christopher D. Manning, Andrew Ng, and Christopher Potts. Recursive deep models for semantic compositionality over a sentiment treebank. In *Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing*, pages 1631–1642, Seattle, Washington, USA, October 2013. Association for Computational Linguistics. URL https://aclanthology.org/D13-1170.

[73] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1):1929–1958, 2014.

[74] Guillaume Staerman. *Functional anomaly detection and robust estimation*. PhD thesis, Institut polytechnique de Paris, 2022.

[75] Guillaume Staerman, Pavlo Mozharovskyi, and Stéphan Clémençon. The area of the convex hull of sampled curves: a robust functional statistical depth measure. In *Proceedings of the 23nd International Conference on Artificial Intelligence and Statistics (AISTATS 2020)*, volume 108, pages 570–579, 2020.

[76] Guillaume Staerman, Pavlo Mozharovskyi, and Stéphan Clémençon. Affine-invariant integrated rank-weighted depth: Definition, properties and finite sample analysis. *arXiv preprint arXiv:2106.11068*, 2021.

[77] John W. Tukey. Mathematics and the picturing of data. In R.D. James, editor, *Proceedings of the International Congress of Mathematicians*, volume 2, pages 523–531. Canadian Mathematical Congress, 1975.

[78] Hongyu Wang, Shuming Ma, Li Dong, Shaohan Huang, Dongdong Zhang, and Furu Wei. Deepnet: Scaling transformers to 1,000 layers. *arXiv preprint arXiv:2203.00555*, 2022.

[79] Adina Williams, Nikita Nangia, and Samuel Bowman. A broad-coverage challenge corpus for sentence understanding through inference. In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers)*, pages 1112–1122, New Orleans, Louisiana, June 2018. Association for Computational Linguistics. doi: 10.18653/v1/N18-1101. URL https://aclanthology.org/N18-1101.

[80] Jim Winkens, Rudy Bunel, Abhijit Guha Roy, Robert Stanforth, Vivek Natarajan, Joseph R. Ledsam, Patricia MacWilliams, Pushmeet Kohli, Alan Karthikesalingam, Simon A. A. Kohl, taylan. cemgil, S. M. Ali Eslami, and Olaf Ronneberger. Contrastive training for improved out-of-distribution detection. *ArXiv*, abs/2007.05566, 2020.

[81] Ruiqi Zhong, Dhruba Ghosh, Dan Klein, and Jacob Steinhardt. Are larger pretrained language models uniformly better? comparing performance at the instance level. *arXiv preprint arXiv:2105.06020*, 2021.

[82] Wenxuan Zhou, Fangyu Liu, and Muhao Chen. Contrastive out-of-distribution detection for pretrained transformers. *arXiv preprint arXiv:2104.08812*, 2021.

[83] Yijun Zuo and Robert Serfling. General notions of statistical depth function. *The Annals of Statistics*, 28(2):461–482, 2000.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes] We have backed all of our claims in the abstract and introduction throughout the work. See the summary of our contributions at Section 1.1.
   (b) Did you describe the limitations of your work? [Yes] Please see Section CITE.
   (c) Did you discuss any potential negative societal impacts of your work? [N/A] Our works aim at developing safer AI systems, so we believe our does not have any negative societal impact.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [N/A]
   (b) Did you include complete proofs of all theoretical results? [N/A]
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] We include extensive instructions to reproduce the main experimental results in both the supplementary material and main paper.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] We provide an extensive analysis on the hyperparamters for training the models and reproducing the results in the supplementary material.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [Yes] We report error bars in all of our main results (please see Sections 5 and 6).
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] We provide a rough estimate of the amount of compute used in the supplementary material.
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] We cite all the datasets we use in the experimental setup of this work in the main paper.
   (b) Did you mention the license of the assets? [N/A] .
   (c) Did you include any new assets either in the supplemental material or as a URL? [Yes] We open-source our code in the supplementary material.
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [N/A] .
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A] .
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]