# Double Trouble: How to *not* explain a text classifier's decisions using counterfactuals synthesized by masked language models?

Anonymous ACL submission

#### Abstract

A principle behind dozens of attribution methods is to take the prediction difference between before-and-after an input feature (here, a token) is removed as its attribution-the individual treatment effect in causal inference. A recent popular Input Marginalization (IM) method (Kim et al., 2020) uses BERT to replace a token—i.e. simulating the do(.) operator yielding more plausible counterfactuals. While Kim et al. (2020) reported that IM is effective, we find this conclusion not convincing as the Deletion<sub>BFRT</sub> metric used in their paper is biased towards IM. Importantly, this bias should exist in many Deletion-based metrics, e.g., Insertion (Arras et al., 2017), Sufficiency, and Comprehensiveness (DeYoung et al., 2020)). Furthermore, our rigorous evaluation using 6 metrics and on 3 datasets finds no evidence that IM is better than a Leave-One-Out (LOO) baseline. We provide two explanations for why IM is not better than LOO: (1) deleting a single word from the input only marginally reduces a classifier's accuracy; and (2) a highly predictable word is always given near-zero attribution which may not match its true importance to the target classifier.

## 1 Introduction

001

012

017

019

024

Feature attribution maps (AMs), i.e. highlights indicating the importance of each input token w.r.t. a classifier's decision, can help improve *human accuracy* on downstream tasks including detecting fake movie reviews (Lai and Tan, 2019) or identifying biases in text classifiers (Liu and Avci, 2019).

Many Leave-One-Out (LOO) methods compute the attribution of an input token by measuring the prediction changes after substituting the token embedding with zeros (Li et al., 2016; Jin et al., 2020) or UNK (Kim et al., 2020). That is, deleting or replacing features is the underlying principle of at least 25 attribution methods (Covert et al., 2020).

Based on evidence in computer vision (Bansal et al., 2020; Zhang et al., 2019), prior works in

(a)	(a) <b>SST</b> – Groundtruth & target class: "positive"					
s	The very definition of the ' small ' movie , but					
3	it is a good stepping stone for director Sprecher.					
	0.9793 stepping 0.9760 stone 0.8712 for					
	0.0050 rolling 0.0048 stones 0.0860 to					
	0.0021 casting 0.0043 point 0.0059,					
D.	The very definition of the 'small' movie, but					
IM <sub>0</sub>	it is a good stepping stone for director Sprecher.					
IM <sub>1</sub>	The very definition of the 'small' movie, but					
11111	it is a good stepping stone for director Sprecher.					
IMa	The very definition of the 'small' movie, but					
11112	it is a good stepping stone for director Sprecher.					
IM <sub>3</sub>	The very definition of the small movie, but					
	it is a good stepping stone for director Sprecher.					
(b)	e-SNLI – Groundtruth & target class: "contradiction"					
(0) ·	A group of people prepare hot air balloons for takeoff.					
1	0.9997 hot 0.9877 air 0.9628 balloons					
	0.0001 compressed 0.0102 water 0.0282 balloon					
	0.0001 compressed 0.0102 water 0.0282 barroon					
1H	0.0000 open 0.0008 helium 0.0019 engines					
H	0.0000 open 0.0008 helium 0.0019 engines A group of people prepare cars for racing .					
	0.0000 open0.0008 helium0.0019 enginesA group of people preparecarsfor racing .A group of people prepare hot air balloons for takeoff .					
IM <sub>0</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people preparecars for racing .					
IM <sub>0</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .					
IM <sub>0</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people preparecars for racing .					
IM <sub>0</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people preparecars for racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .					
IM <sub>0</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people prepare carsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare carsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare carsFor racing .					
IM <sub>0</sub> IM <sub>1</sub> IM <sub>2</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people preparecarsfor racing .A group of people prepare hot air balloons for takeoff .A group of people preparecarsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare carsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare cars for racing .					
IM <sub>0</sub> IM <sub>1</sub> IM <sub>2</sub>	0.0000 open0.0008 helium0.0019 enginesA group of people prepare carsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare carsfor racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .A group of people prepare cars for racing .A group of people prepare hot air balloons for takeoff .A group of people prepare hot air balloons for takeoff .					

Figure 1: Color map: negative -1, neutral 0, positive +1. Many words labeled important by humans such as "stepping", "stone" (in SST) or "hot", "air" (in e-SNLI) are always given near-zero attribution by IM (because they are highly predictable by BERT, e.g. 0.9793 for stepping) regardless of the classifier's parameters. Even when randomizing the classifier's weights three times, the IM attribution of these words remains unchanged at near zero (IM<sub>1</sub> to IM<sub>3</sub>). Therefore, when marginalizing over the top-k BERT candidates (e.g., "stepping", "rolling", "casting"), the IM attribution for low-entropy words tends to zero, leading to heatmaps that are biased, less accurate, and less plausible than LOO<sub>empty</sub>.

NLP *hypothesized* that removing a word from an input text forms out-of-distribution (OOD) inputs that yield erroneous AMs (Kim et al., 2020; Har-

becke and Alt, 2020) or AMs inconsistent with human's perception of causality (Hase et al., 2021). To generate plausible counterfactuals, two teams of researchers (Kim et al., 2020; Harbecke and Alt, 2020) proposed Input Marginalization (IM), i.e. replace a word using BERT (Devlin et al., 2019) and compute an average prediction difference by marginalizing over all predicted words. Kim et al. (2020) claimed that IM yields more accurate AMs than the baselines that replace words by UNK or zeros but their quantitative results were reported for only  $one^1$  dataset and *one* evaluation metric.

047

048

061

067

072

080

086

090

In this paper, we re-assess their claim by, first, reproducing their IM results<sup>2</sup>, and then rigorously evaluating the effectiveness of IM on a diverse set of *three* datasets and *six* metrics. We found that:

- The Deletion<sub>BERT</sub> metric in Kim et al. (2020) is biased towards IM as both use BERT to replace words (Sec. 4). In contrast, the original Deletion metric (Arras et al., 2017) favors the LOO<sub>empty</sub> baseline as both delete words. This bias causes the incorrect interpretation that IM is better than LOO baselines in Kim et al. (2020) and exists in all Deletion variants including Insertion (Arras et al., 2017), Sufficiency, and Comprehensiveness (DeYoung et al., 2020).
- Under ROAR & ROAR<sub>BERT</sub> (Hooker et al., 2019), the metrics that correct for the distribution shift in Deletion, LOO<sub>empty</sub> outperforms IM (Sec. 5.1). Compared to human annotations, LOO<sub>empty</sub> generates more plausible explanations than IM (Sec. 5.2). Under sanity check (Adebayo et al., 2018), IM is worse than LOO<sub>empty</sub> (Sec. 5.3). Overall, we find **no evidence that IM is better** than a simple LOO<sub>empty</sub> baseline on any of the above *four* metrics (which exclude the biased Deletion & Deletion<sub>BERT</sub>).
- To further test the main idea of IM—whether using BERT to generate plausible counterfactuals improves explainability—we integrate BERT into LIME (Ribeiro et al., 2016) but find that LIME<sub>BERT</sub> only performs similarly to the original LIME (Sec. 6).

We argue that IM is not effective in practice because: (1) deleting a single word from an input has only a marginal effect to classification accuracy (Sec. 7.1); and (2) given a *perfect*, masked language model G, IM would be still **unfaithful** because highly predictable words according to G, e.g. "hot", "air" in Fig.1, are always assigned near-zero attribution in IM *regardless* of how important they are to the classifier (Sec. 7.2). To our knowledge, our work is the first to question the commonly-assumed effectiveness of IM in NLP.

093

094

095

100

101

102

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

## 2 Methods and Related Work

Let  $f : \mathbb{R}^{n \times d} \to [0, 1]$  be a text classifier that maps a sequence x of n token embeddings, each of size d, onto a confidence score of an output label. An attribution function A takes three inputs—a sequence x, the model f, and a set of hyperparameters  $\mathcal{H}$  and outputs a vector  $a = A(f, x, \mathcal{H}) \in [-1, 1]^n$ . Here, the explanation a associates each input token  $x_i$  to a scalar  $a_i \in [-1, 1]$ , indicating how much  $x_i$ contributes for or against the target label.

**Leave-One-Out** (LOO) is a well-known method (Li et al., 2016) for estimating the attribution  $a_i$ by computing the confidence-score change after a token  $x_i$  is left out of the input x, creating a shorter sequence  $x_{-i}$ :

$$a_i = f(\boldsymbol{x}) - f(\boldsymbol{x}_{-i}) \tag{1}$$

This "prediction difference" (Robnik-Šikonja and Kononenko, 2008) is widely used as attribution in LOO methods (a.k.a "occlusion") in both NLP (Jin et al., 2020) and Computer Vision (CV).

Under Pearl (2009) causal framework, the attribution  $a_i$  in Eq. 1 relies on a single, unrealistic counterfactual  $x_{-i}$  and thus is a biased estimate of the individual treatment effect (ITE):

$$ITE = f(\boldsymbol{x}) - \mathbb{E}[f(\boldsymbol{x}) \mid do(T=0)] \quad (2)$$

where the binary treatment T, here, is to keep or "realistically remove" the token  $x_i$  (i.e. T = 1 or 0) in the input x, prior to the computation of f(x).

**Removal techniques** In CV, earlier attribution methods erase a feature by replacing it with (a) zeros (Zeiler and Fergus, 2014; Ribeiro et al., 2016); (b) random noise (Dabkowski and Gal, 2017; Lundberg and Lee, 2017); or (c) blurred versions of the original content (Fong et al., 2019). Yet, these handdesigned perturbation methods produce unrealistic counterfactuals that make AMs more unstable and less accurate (Bansal et al., 2020).

<sup>&</sup>lt;sup>1</sup>No quantitative results on SNLI, only SST-2.

<sup>&</sup>lt;sup>2</sup>Code and pre-trained models are available at https://anonymizedForReview.

185

186

187

139Recent works proposed to simulate the do(T = 0) operator using an image inpainter. How-1400) operator using an image inpainter. How-141ever, they either generate unnatural counterfactuals142(Chang et al., 2019; Goyal et al., 2019) or only a143single, plausible counterfactual per example (Agar-144wal and Nguyen, 2020).

145

146

147

148

149

150

152

153

155

156

157

158

159

162

163

164

165

166

168

169

170

171

177

178

179

180

**Input marginalization (IM)** In the parallel world of NLP, IM offers the closest estimate of the ITE. They compute the expectation term in Eq. 2 by marginalizing over many plausible textual counterfactuals generated by BERT:

$$\mathbb{E}[f(\boldsymbol{x}) \mid do(T=0)] = \sum_{\tilde{x}_i \in \mathcal{V}} p(\tilde{x}_i | \boldsymbol{x}_{-i}) \cdot f(\boldsymbol{x}_{-i}, \tilde{x}_i) \quad (3)$$

where  $\tilde{x}_i$  is a token suggested by BERT (e.g., "hot", "compressed", or "open" in Fig. 1) with a likelihood of  $p(\tilde{x}_i | \boldsymbol{x}_{-i})$  to replace the masked token  $x_i$ .  $\mathcal{V}$  is the BERT vocabulary of 30,522 tokens.  $f(\boldsymbol{x}_{-i}, \tilde{x}_i)$ is the classification probability when token  $x_i$  in the original input is replaced with  $\tilde{x}_i$ .

IM attribution is in the  $\log$  space:

$$a_{\text{IM}} = \log \text{-} \text{odds}(f(\boldsymbol{x})) - \log \text{-} \text{odds}(\mathbb{E}[f(\boldsymbol{x}) \mid do(T=0)]) \quad (4)$$

where  $\log - \text{odds}(p) = \log_2(p/(1-p))$ .

As computing the expectation term (Eq. 3) over the full vocabulary of size  $\sim 30$ K is prohibitively slow, the authors only marginalized over the words that have a likelihood  $\geq 10^{-5}$ . We are *able to reproduce* the IM results of (Kim et al., 2020) by taking only the top-10 words and thus we use this setup for all experiments. Note that under BERT, the top-10 tokens, on average, already account for 81%, 90%, and 92% of the probability mass for SST-2, e-SNLI, and MultiRC, respectively.

BERT Like Kim et al. (2020), we use a pretrained BERT "base", uncased model (Devlin et al.,
2019), from Huggingface (2020), to fill in a MASK
token to synthesize plausible counterfactuals.

**LIME** We also test our findings of IM by integrating BERT into LIME, i.e. a more accurate attribution method (compared to LOO), which masks out multiple tokens at once to compute attribution.

181LIME generates a set of randomly masked ver-182sions of the input, and the attribution of a token183 $x_i$ , is effectively the mean classification probability184over all the masked inputs when  $x_i$  is not masked

out. On average, each original LIME counterfactual has 50% of tokens taken out, often yielding text with large syntactic and grammatical errors.

**LIME**<sub>BERT</sub> We use BERT to replace multiple masked tokens<sup>3</sup> in each masked sentence generated by LIME to construct more plausible counterfactuals. However, for each word, we only use the top-1 highest-likelihood token given by BERT instead of marginalizing over multiple tokens because (1) the full marginalization is prohibitively slow; and (2) the top-1 token already carries most of the weight  $(p \ge 0.81$ ; see Table 6).

#### **3** Experiment framework

# 3.1 Three datasets

We select a diverse set of three classification datasets that enable us to (1) compare with the results reported by Kim et al. (2020); and (2) assess AMs on six evaluation metrics (described in Sec. 3.3). These three tasks span from sentiment analysis (SST-2), natural language inference (e-SNLI) to question answering (MultiRC), covering a wide range of sequence length (~20, 24, and 299 tokens per example, respectively). SST-2 and e-SNLI were the two datasets where Kim et al. (2020) found IM to be superior to LOO baselines.

**SST** Stanford Sentiment Treebank (Socher et al., 2013) is a dataset of ~12K RottenTomato moviereview *sentences*, which contain human-annotated sentiment annotations for phrases. Each phrase and sentence in SST is assigned a sentiment score  $\in [0, 1]$  (0 = negative, 0.5 = neutral, 1 = positive).

**SST-2** has  $\sim$ 70K SST examples (including both phrases and sentences) where the regression scores per example were binarized to form a binary classification task (Socher et al., 2013).

**e-SNLI** A 3-way classification task of detecting whether the relation between a premise and a hypothesis is entailment, neutral or contradiction (Bowman et al., 2015). e-SNLI has 569K instances of (input, label, explanation) where the explanations are crowd-sourced (Camburu et al., 2018).

**MultiRC** Multi-sentence Reading Comprehension (Khashabi et al., 2018) is a multiple-choice question-answering task that provides multiple input sentences as well as a question and asks the

 $<sup>^{3}</sup>$ We find replacing all tokens at once or one at a time to produce similar LIME<sub>BERT</sub> results.

230 231

- 233 234

241

242

243

245

246

247

249

251

252

256

258

259

261

262

263

267

model to select one or multiple correct answer sentences. MultiRC has  $\sim 6K$  examples with humanannotated highlights at the sentence level.

# 3.2 Classifiers

Following Kim et al. (2020); Harbecke and Alt (2020); Hase et al. (2021), we test IM and LOO baselines in explaining BERT-based classifiers.

For each task, we train a classifier by fine-tuning the entire model, which consists of a classification layer on top of the pre-trained BERT (described in Sec. 2). The dev-set top-1 accuracy scores of our SST-2, e-SNLI, & MultiRC classifiers are 92.66%, 90.92%, and 69.10%, respectively. On the SST binarized dev-set, which contains only sentences, the SST-2-trained classifier's accuracy is 87.83%.

**Hyperparameters** Following the training scheme of HuggingFace, we fine-tune all classifiers for 3 epochs using Adam optimizer (Kingma and Ba, 2015) with a learning rate of 0.00002,  $\beta_1$ = 0.9,  $\beta_2$  = 0.999,  $\epsilon = 10^{-8}$ . A batch size of 32 and a max sequence length of 128 are used for SST-2 and e-SNLI while these hyperparameters for MultiRC are 8 and 512, respectively. Dropout with a probability of 0.1 is applied to all layers. Each model was trained on an NVIDIA 1080Ti GPU.

## 3.3 Six evaluation metrics

As there are *no groundtruth* explanations in XAI, we use six common metrics to rigorously assess IM's effectiveness. For each classifier, we evaluate the AMs generated for all dev-set examples.

**Deletion** is similar to "Comprehensiveness" (DeYoung et al., 2020) and is based on the idea that deleting a token of higher importance from the input should cause a larger drop in the output confidence score. We take the original input and delete one token at a time until 20% of the tokens in the input is deleted. A more accurate explanation is expected to have a lower Area Under the output-probability Curve (AUC) (Arras et al., 2017).

269Deletion<sub>BERT</sub>a.k.a. AUC<sub>rep</sub> in Kim et al. (2020),270is the Deletion metric but where a given token is271replaced by a BERT top-1 suggestion instead of272an empty string. Deletion<sub>BERT</sub> was proposed to273minimize the OOD-ness of samples (introduced by274deleting words in the original Deletion metric), i.e.275akin to integrating BERT into LOO to create IM.

276 RemOve And Retrain (ROAR) To avoid a potential OOD generalization issue caused by the
278 Deletion metric, a common alternative is to retrain

the classifier on these modified inputs (where N% of the highest-attribution words are deleted) and measure its accuracy drop (Hooker et al., 2019). A more faithful attribution method is supposed to lead to a re-trained classifier of lower accuracy as the more important words have been deleted from the training examples. For completeness, we also implement **ROAR**<sub>BERT</sub>, which uses BERT to replace the highest-attribution tokens<sup>4</sup> instead of deleting them without replacement.

279

280

281

282

283

284

285

286

288

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

**Agreement with human-annotated highlights** To assess the plausibility of AMs to serve as a text-highlighter, a common metric is to compare an AM with the tokens that humans deem indicative of the groundtruth label (Wiegreffe and Marasović, 2021).

Because human annotators only label the tokens supportive of a label (e.g. Fig. 2), when comparing AMs with human annotations, we zero out the negative values in AMs. Following Zhou et al. (2016), we binarize a resulting AM at an optimal threshold  $\tau$  in order to compare it with humanannotated highlights under Precision@1.

**Sanity check** (Adebayo et al., 2018) is a wellknown metric for testing insensitivity (i.e. bias) of attribution methods w.r.t. model parameters. For ease of interpretation, we compute the % change of per-word attribution values in *sign* and *magnitude* as we randomize the classification layer's weights. A better attribution method is expected to be more sensitive to weight randomization.

# **4** Bias of Deletion metric and its variants

In explaining SST-2 classifiers, we successfully reproduce the AUC<sub>rep</sub> results reported in Kim et al. (2020), i.e. IM outperformed LOO<sub>zero</sub> and LOO<sub>unk</sub>, which were implemented by replacing a word with the PAD and UNK token of BERT, respectively (Table 1). However, we hypothesize that Deletion<sub>BERT</sub> is biased towards IM as both use BERT to replace words, yielding a false sense of IM effectiveness reported in Kim et al. (2020).

To test this hypothesis, we add another baseline of  $LOO_{empty}$ , which was *not* included in Kim et al. (2020), i.e. erasing a token from the input without replacement (Eq. 1), mirroring the original Deletion metric. To compare with IM, all LOO methods in this paper are also in the log-odds space.

**Results** Interestingly, we find that, under Deletion,

 $<sup>^4</sup>$ The chance that a sentence remains unchanged after BERT replacement is low,  $\leq 1\%$ .

on both SST-2 and e-SNLI, IM *underperformed all* three LOO baselines and that LOO<sub>empty</sub> is the highest-performing method (Table 1). In contrast, IM is the best method under Deletion<sub>BERT</sub>. To our knowledge, our work is **the first to document this bias** of the Deletion metric **widely used in the literature** (Hase et al., 2021; Wiegreffe and Marasović, 2021; Arras et al., 2017). This bias, in principle, should also **exist in other Deletion variants** including Insertion (Arras et al., 2017), Sufficiency, and Comprehensiveness (De Young et al., 2020).

327

328

331

332

333

337

338

339

341

342

343

345

347

351

357

361

Task	Metrics ↓	IM	$\text{LOO}_{\text{zero}}$	$\mathrm{LOO}_{unk}$	$\text{LOO}_{\text{empty}}$
SST-2	Deletion	0.4732	0.4374	0.4464	0.4241
	DeletionBERT	0.4922	0.4970	0.5047	0.5065
e-SNLI	Deletion	0.3912	0.2798	0.3742	0.2506
	DeletionBERT	0.2816	0.3240	0.3636	0.3328

Table 1: IM is the **best** method under Deletion<sub>BERT</sub>, as reported in Kim et al. (2020), but the **worst** under Deletion. Both metrics measure AUC (lower is better).

# 5 No evidence that IM is better than LOO

To avoid the critical bias of Deletion and Deletion<sub>BERT</sub>, we further compare IM and LOO on **four** common metrics that are not Deletion-based.

# 5.1 Under ROAR and ROAR<sub>BERT</sub>, IM is on-par with or worse than LOO<sub>empty</sub>

A lower AUC under Deletion may be the artifact of the classifier misbehaving under the distribution shift when one or multiple input words are deleted. ROAR (Hooker et al., 2019) was designed to ameliorate this issue by re-training the classifier on the modified training-set (where the top N% highest-attribution tokens in each example are deleted) before evaluating their accuracy.

To more objectively assess IM, we use ROAR and ROAR<sub>BERT</sub> metrics to compare IM vs. LOO<sub>empty</sub> (i.e. the best LOO variant in Table 1). **Experiment** For both IM and LOO<sub>empty</sub>, we generate AMs for every example in the SST-2 train and dev sets, and remove N% highest-attribution tokens per example to create new train and dev sets. We train 5 models on the new training set and evaluate them on the new dev set. We repeat ROAR and ROAR<sub>BERT</sub> with  $N \in \{10, 20, 30\}$ .<sup>5</sup> **Results** As more tokens are removed (i.e. N increases), the mean accuracy of 5 models gradually decreases (Table 2; from 92.66% to ~67%). Under both ROAR and ROAR<sub>BERT</sub>, the models trained on the new training set derived from LOO<sub>empty</sub> AMs often obtain lower mean accuracy than those of IM (Table 2a vs. b). At N = 10% under ROAR, **LOO**<sub>empty</sub> **outperforms IM** (Table 2; 74.59 vs. 76.22), which is statistically significant (2-sample *t*-test, p = 0.037). In all other cases, the difference between IM vs. LOO<sub>empty</sub> is not statistically significant.

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

378

379

380

381

382

383

384

385

386

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

In sum, under both ROAR and ROAR<sub>BERT</sub>, IM is *not more faithful* than  $LOO_{empty}$ .

# **5.2** LOO<sub>empty</sub> explanations are better aligned with human annotations than IM

To increase our understanding of the differences between  $LOO_{empty}$  and IM, here, we compare them against the human highlights for SST, e-SNLI, and MultiRC. While human highlights are not exactly groundtruth explanations, this human-alignment metric is a common proxy for the correctness of AMs in both NLP (Wiegreffe and Marasović, 2021) and computer vision (Zhou et al., 2016).

Annotation preprocessing To control for quality, we preprocess the human annotations in each dataset as the following. In SST, where each sentence has multiple phrases labeled with a sentiment score  $\in [0, 1]$  (0.5 being the "neutral" midpoint), we only use the phrases that have high-confidence sentiment scores, i.e.  $\leq 0.3$  (for "negative") or  $\geq 0.7$  (for "positive"). Also, we do not use the annotated phrases that are too long, i.e., longer than 50% of the sentence length.

Each token in an e-SNLI example are labeled "important" by between 0–3 annotators. To filter out noise, we only use the tokens that are highlighted by *at least* two or three annotators (hereafter "L2" and "L3" subsets, respectively).

A MultiRC example contains a question and a paragraph where each sentence is labeled "important" or "unimportant" to the groundtruth answer (Fig. A5). We convert these sentence-level highlights into token-level highlights to compare them with the binarized AMs of IM and LOO<sub>empty</sub>. **Experiment** We run IM and LOO<sub>empty</sub> on the BERT-based classifiers on the dev set of SST, e-SNLI, and MultiRC. All AMs generated are binarized using a threshold  $\tau \in \{0.05x \mid 0 < x < 20 \text{ and } x \in \mathbb{N}\}$ . We compute the average IoU, pre-

<sup>&</sup>lt;sup>5</sup>We do not use  $N \ge 40$  because: (1) according to SST human annotations, only 37% of the tokens per example are labeled "important" (Table A2c); and (2) SST-2 examples are short and may contain as few as 4 tokens per example.

Accuracy in % (lo	ower is better)	ROAR			ROAR <sub>BERT</sub>			
Method	N=0%	10%	20%	30%	10%	20%	30%	
(a) LOO <sub>empty</sub>	$92.62\pm0.30$	$\textbf{74.59} \pm 0.78$	$\textbf{68.94} \pm 1.46$	$67.89\pm0.79$	$\textbf{76.79} \pm 0.56$	$71.95\pm0.75$	$\textbf{67.62} \pm 1.16$	
(b) IM	$92.62\pm0.30$	$76.22 \pm 1.18$	$70.07\pm0.69$	$\textbf{66.54} \pm 1.89$	$77.36 \pm 0.90$	$\textbf{71.56} \pm 1.55$	$67.68 \pm 0.96$	
(c) Random	$92.62\pm0.30$	$89.22 \pm 0.53$	$87.75 \pm 0.19$	$85.62\pm0.53$	$89.38 \pm 0.47$	$88.23 \pm 0.31$	$85.21\pm0.47$	
(d) <i>t</i> -test p-value	N/A	0.0370	0.1740	0.1974	0.2672	0.6312	0.9245	

Table 2: Dev-set mean accuracy (%) of 5 models trained on the new SST-2 examples where N% of highestattribution words per example are removed (i.e. ROAR) or replaced via BERT (i.e. ROAR<sub>BERT</sub>). On average, under both metrics, LOO<sub>empty</sub> (a) is a slightly better, i.e. lower mean accuracy, than IM (b). Notably, LOO<sub>empty</sub> statistically significantly outperforms IM under ROAR at N = 10% (2-sample t-test; p = 0.037) (d). Both LOO<sub>empty</sub> and IM substantially outperform a random baseline (c) that considers N% random tokens important.

Metric ↑		(a) SST			(b) e-S	SNLI L2	(c) e-S	SNLI L3	(d) N	AultiRC	
Higher is better	IM	LOO <sub>empty</sub>	LIME	LIMEBERT	LIME <sub>BERT_SST</sub>	IM	LOO <sub>empty</sub>	IM	LOO <sub>empty</sub>	IM	LOO <sub>empty</sub>
IoU	0.2377	0.2756	0.3193	0.3170	0.3127	0.3316	0.3415	0.2811	0.3411	0.0437	0.0887
precision	0.5129	0.4760	0.4831	0.4629	0.4671	0.4599	0.4867	0.3814	0.4687	0.1784	0.1940
recall	0.5245	0.6077	0.6882	0.7000	0.6886	0.6085	0.6158	0.5699	0.5875	0.0630	0.2876
F1	0.5186	0.5338	0.5677	0.5573	0.5566	0.5239	0.5437	0.4570	0.5214	0.0931	0.2317

Table 3: Compared to IM, LOO<sub>empty</sub> is substantially more consistent with human annotations over all three datasets. Note that the gap between  $LOO_{empty}$  and IM is  $\sim 3 \times$  wider when comparing AMs with the e-SNLI tokens that at least three annotators label "important" (i.e. L3), compared to L2 (higher is better). LIME<sub>BERT</sub> explanations are slightly less consistent with human highlights than those of LIME (a) despite their counterfactuals are more realistic.

cision, recall, and F1 over pairs of (human binary 412 map, binarized AM) and report the results at the 413 optimal  $\tau$  of each explanation method. For both  $LOO_{empty}$  and IM,  $\tau = 0.1$  on SNLI-L2 and 0.05 415 on both SST-2 and MultiRC. On SNLI-L3,  $\tau$  is 416 0.40 and 0.45 for LOO<sub>empty</sub> and IM, respectively. SST results We found that LOO<sub>empty</sub> aligns bet-418 ter with human highlights than IM (Figs. 2 & A7). 419 LOO<sub>empty</sub> outperforms IM in both F1 and IoU 420 scores (Table 3a; 0.2756 vs 0.2377) with a notably 422 large recall gap (0.6077 vs. 0.5245).

414

417

421

423

424

SST	SST Groundtruth & Prediction: "positive" movie review					
Input	Mr. Tsai <mark>is a very original artist in his</mark> medium , and What Time Is It There ?					
IM	Mr. <mark>Tsai</mark> is a very <mark>original</mark> artist in his <mark>medium</mark> , and What Time Is It <mark>There</mark> ?					
	IoU: 0.17, precision: 0.33, recall: 0.25					
LOO	Mr. Tsai is a very original artist in his medium, and What Time Is It There ?					
	IoU: 0.80, precision: 0.80, recall: 1.00					

Figure 2: LOO<sub>empty</sub> binarized attribution maps align better with human highlights than those of IM.

e-SNLI and MultiRC results Similarly, in both tasks, LOO<sub>empty</sub> explanations are more consistent with human highlights than IM explanations under all four metrics (see Table 3b-d and qualitative examples in Figs. 3 & A8–A11).

425

426

427

428

429

430

431

432

Remarkably, in MultiRC where each example is substantially longer (~299 tokens per example) than those in the other tasks, the recall and F1 scores of LOO<sub>empty</sub> is, respectively,  $2 \times$  and  $4 \times$ higher than those of IM (see Table 3).

e-SN	LI example. Groundtruth & Prediction: "entailment"
Р	Two men dressed in black practicing martial arts
1	on a gym floor .
Η	Two men are doing martial arts.
IM	Two men dressed in black practicing martial arts
	on a gym floor .
	Two men are doing martial arts .
	IoU: 0.09, precision: 0.17, recall: 0.16
LOO	Two men dressed in black practicing martial arts
LOO	on a gym floor .
	Two men are doing martial arts .
	IoU: 0.50, precision: 0.56, recall: 0.83

Figure 3: LOO<sub>empty</sub> important words are in a stronger agreement with human highlights. Each e-SNLI example contains a pair of premise (P) and hypothesis (H).

# 

### 5.3 IM less sensitive to model randomization

Adebayo et al. (2018) found that many attribution methods can be surprisingly biased, i.e. *insensitive* to even randomization of the classifier's parameters. Here, we test the degree of insensitivity of IM when the last classification layer of BERT-based classifiers is randomly re-initialized. We use three SST-2 classifiers and three e-SNLI classifiers.

Surprisingly, IM is consistently worse than  $LOO_{empty}$ , i.e. more insensitive to classifier randomization. That is, on average, the IM attribution of a word changes signs (from positive to negative or vice versa) less frequently, e.g. 62.27% of the time, compared to 71.41% for  $LOO_{empty}$ on SST-2 (Table 4a). The average change in attribution *magnitude* of IM is also ~1.5× smaller than that of  $LOO_{empty}$  (Table 4b). For example, the IM attribution of "hot", "air", "balloon", and "racing" in Fig. 1 remain consistently **unchanged near-zero even when the classifier is randomized three times** because these words are highly predictable by BERT from the context (Fig. 1b;  $IM_1$  to  $IM_3$ ). More in-depth explanations in Sec. 8.

Criteria	Method	SST-2	e-SNLI	
(a) % tokens	$\text{LOO}_{\text{empty}}$	$\textbf{71.41} \pm 17.12$	$\textbf{56.07} \pm 21.82$	
changing sign	IM	$62.27\pm17.75$	$49.57\pm20.35$	
(b) Average	LOO <sub>empty</sub>	$\textbf{0.46} \pm 0.18$	<b>0.26</b> ± 0.14	
absolute of differences	IM	$0.31\pm0.12$	$0.16\pm0.12$	

Table 4: The percentage (%) of token (a) whose attribution scores change signs and (b) the average of absolute differences in attribution magnitude after classifier randomization (higher is better). IM is consistently more insensitive than  $LOO_{empty}$  in both SST-2 and e-SNLI.

# 6 LIME<sub>BERT</sub> attribution maps are *not* more aligned with human annotations

Sec. 5 shows that replacing **a single word** by BERT (instead of deleting) creates more *realistic* inputs but does *not* improve AM quality w.r.t. LOO.

Here, we test whether this conclusion generalizes to the case of LIME where **multiple words** are deleted from a sentence. Similar to Sec. 5.2, we compare LIME and LIME<sub>BERT</sub> AMs with human SST annotations (but not the Deletion-derived metrics due to their bias described in Sec. 4).

**Experiment** We use the default hyperparameters of the original LIME (Ribeiro, 2021) for both LIME and LIME<sub>BERT</sub>. The number of counterfactual samples was 1,000 per example.

**Results** Although LIME<sub>BERT</sub> counterfactuals are more natural, the derived explanations are surprisingly less plausible to human than those generated by the original LIME. That is, compared to human annotations in SST, LIME<sub>BERT</sub>'s IoU, precision and F1 scores are all slightly worse than those of LIME (Table 3a). Consistent with the IM vs. LOO<sub>empty</sub> comparison in Sec. 5.2, replacing one or more words (instead of deleting them) using BERT in LIME generates AMs that are similarly or less aligned with humans. In sum, for both LOO and LIME, we find no evidence that using realistic counterfactuals from BERT provides improvement in AM quality.

To minimize the possibility that the pre-trained BERT is suboptimal in predicting missing words on SST-2, we also finetune BERT using the mask-language modeling objective on SST-2 and repeat the experiment in this section. Yet, interestingly, we find the above conclusion to not change (Table 3a; LIME<sub>BERT\_SST</sub> is worse than LIME).

# 7 Why is IM not better than LOO<sub>empty</sub>?

Despite being  $\geq 5 \times$  more computationally expensive<sup>6</sup>, IM is not better than LOO<sub>empty</sub> on all four unbiased tested metrics (Sec. 5). We provide two explanations for this surprising finding.

# 7.1 Classification accuracy only drops marginally when a token is removed

Prior works argue that feeding unnatural LOO samples into classifiers may yield more unfaithful AMs (Kim et al., 2020; Harbecke and Alt, 2020; Hase et al., 2021); however, our rigorous evaluation using 3 datasets and 6 evaluation metrics **did not find any case** where IM outperforms LOO (except under the biased Deletion<sub>BERT</sub> metric).

To understand why using more plausible samples did not improve AM explainability, we assess the  $\Delta$  drop in classification accuracy when a word is deleted (i.e., LOO<sub>empty</sub> samples; Fig. A12) and the  $\Delta$  when a word is replaced using BERT (i.e. IM samples).

**Results** Across SST, e-SNLI, and MultiRC, the accuracy scores of classifiers only drop marginally  $\sim$ 1-4% (Table 5) when a single token is deleted.

 $<sup>^6</sup>$ On a 1080Ti GPU, it took IM  ${\sim}15$  mins to complete the full SST dev-set compared to  ${\sim}3$  mins for LOO<sub>empty</sub>. These numbers are  ${\sim}105$  hrs vs.  ${\sim}10.5$  hrs on the MultiRC dev-set.

See Figs. A12 & A13 for qualitative examples that removing a single token hardly changes the predicted label. Whether a word is removed or replaced by BERT is almost unimportant in tasks with long examples such as MultiRC (Table 5; 1.10% and 0.24%). In sum, we do not find the unnaturalness of LOO samples to substantially hurt model performance, questioning the need raised in (Hase et al., 2021; Harbecke and Alt, 2020; Kim et al., 2020) for realistic counterfactuals.

515

516

517

518

520

521

524

525

526

527

528

530

534

535

536

537

538

539

541

Drop in accuracy (%)	SST	e-SNLI	MultiRC
(a) LOO <sub>empty</sub> samples	3.52	4.92	1.10
(b) IM samples	2.20	4.86	0.24

Table 5: The dev-set accuracies on SST, e-SNLI and MultiRC (87.83%, 90.92%, and 69.10%, respectively) only drop marginally, here  $\sim$ 1–4 point when a single token is removed (a) or replaced using BERT (b).

# 7.2 By design, IM always assigns near-zero attribution to high-likelihood words regardless of classifiers

We observe that IM scores a substantially lower recall compared to  $LOO_{empty}$  (e.g. 0.0630 vs. 0.2876; Table 3d). That is, IM tends to incorrectly assign too small of attribution to important tokens. Here, we test whether this low-recall issue is because BERT is highly accurate at predicting a single missing word from the remaining text and therefore assigns a high likelihood to such words in Eq. 3, causing low IM attribution in Eq. 2.

**Experiment** For each example in all three datasets, we replaced a single word by BERT's top-1 highest-likelihood token and measured its likelihood and whether the replacement is the same as the original word.

**Results** Across SST, e-SNLI, and MultiRC, the 542 top-1 BERT token matches exactly the original 543 word  $\sim 49, 60, 65\%$  of the time, respectively (Table 6a). This increasing trend of exact-match frequency (from SST, e-SNLI  $\rightarrow$  MultiRC) is consistent with 546 the example length in these three datasets, which 547 is understandable as a word tends to be more pre-548 dictable given a longer context. Among the tokens that human annotators label "important", this 550 exact-match frequency is similarly high (Table 6b). 551 Importantly, the average likelihood score of a top-1 552 exact-match token is high,  $\sim 0.81-0.86$  (Table 6c). See Fig. 1 & Figs. A1–A6 for qualitative examples.

Our findings are aligned with IM's low recall. That is, if BERT fills in an exact-match  $\tilde{x}_i$  for an original word  $x_i$ , the prediction difference for this replacement  $\tilde{x}_i$  will be 0 in Eq. 4. Furthermore, a high likelihood of ~0.81 for  $\tilde{x}_i$  sets an **empirical upper-bound of 0.19 for the attribution of the word**  $x_i$ , which explains the insensitivity of IM to classifier randomization (Fig. 1; IM<sub>1</sub> to IM<sub>3</sub>).

% exact-match (uncased)	SST	e-SNLI	MultiRC
(a) over all tokens	48.94	59.43	64.78
(b) over human highlights	41.25	42.74	68.55
(c) Top-1 word's likelihood	0.8229	0.8146	0.8556

Table 6: Top-1 likelihood scores (c) are the mean likelihood given by BERT for the top-1 predicted words that exactly match the original words (a).

The analysis here is also consistent with our additional findings that IM attribution tends to be smaller than that of LOO<sub>empty</sub> and therefore leads to heatmaps of lower coverage of the words labeled "important" by humans (see Sec. A).

## 8 Discussion and Conclusion

Our series of rigorous experiments reveal severe shortcomings of IM in prior work (Kim et al., 2020; Harbecke and Alt, 2020) for explaining a classifier's decisions in NLP at the *word* level. Consider an example: In the input text, there exists a token  $x_i$ that is ~100% predictable by BERT from the context, i.e.  $p(\tilde{x}_i | \mathbf{x}_{-i}) \approx 1$  (see hot, air or balloons in Fig. 1). Then, by applying Equations 3 & 4, the attribution  $a_i \approx 0$ , by construction, regardless of how important the token  $x_i$  is to the classifier.

A solution may be to leave such  $x_i$  token out of the marginalization (Eq. 3), i.e. only marginalizing over the other tokens suggested by BERT. However, these other replacement tokens altogether have a sum likelihood of 0. That is, replacing token  $x_i$ by zero-probability tokens (i.e. truly implausible) would effectively generate OOD text, which, in turn is not desired (Hase et al., 2021).

Another possible fix for IM in NLP might be to operate at the *phrase* level instead of word level as deleting a set of contiguous words has a larger effect to the classifier predictions. However, in general, using a black-box generative model in the process of explaining the decision of another blackbox classifier may be "Double Trouble" in any domain (Rudin, 2019). 562

555

556

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

590

591

592

593

594

563

### References

595

596

597

598

599

613

614

615

616

617

620

622

623

624

629

632

636

637

638

640

641

642

645

649

- Julius Adebayo, Justin Gilmer, Michael Muelly, Ian Goodfellow, Moritz Hardt, and Been Kim. 2018. Sanity checks for saliency maps. In *Advances in Neural Information Processing Systems*, volume 31. Curran Associates, Inc.
  - Chirag Agarwal and Anh Nguyen. 2020. Explaining image classifiers by removing input features using generative models. In *Proceedings of the Asian Conference on Computer Vision*.
- Leila Arras, Grégoire Montavon, Klaus-Robert Müller, and Wojciech Samek. 2017. Explaining recurrent neural network predictions in sentiment analysis. *EMNLP 2017*, page 159.
- Naman Bansal, Chirag Agarwal, and Anh Nguyen. 2020. Sam: The sensitivity of attribution methods to hyperparameters. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 8673–8683.
- Samuel R. Bowman, Gabor Angeli, Christopher Potts, and Christopher D. Manning. 2015. A large annotated corpus for learning natural language inference. In *Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. Association for Computational Linguistics.
- Oana-Maria Camburu, Tim Rocktäschel, Thomas Lukasiewicz, and Phil Blunsom. 2018. e-snli: Natural language inference with natural language explanations. In Advances in Neural Information Processing Systems, volume 31. Curran Associates, Inc.
- Chun-Hao Chang, Elliot Creager, Anna Goldenberg, and David Duvenaud. 2019. Explaining image classifiers by counterfactual generation. In *International Conference on Learning Representations*.
- Ian Covert, Scott Lundberg, and Su-In Lee. 2020. Feature removal is a unifying principle for model explanation methods. *arXiv preprint arXiv:2011.03623*.
- Piotr Dabkowski and Yarin Gal. 2017. Real time image saliency for black box classifiers. In Advances in Neural Information Processing Systems, pages 6967– 6976.
- Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. 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.
- Jay DeYoung, Sarthak Jain, Nazneen Fatema Rajani, Eric Lehman, Caiming Xiong, Richard Socher, and Byron C. Wallace. 2020. ERASER: A benchmark to evaluate rationalized NLP models. In *Proceedings* of the 58th Annual Meeting of the Association for Computational Linguistics, pages 4443–4458, Online. Association for Computational Linguistics.

Ruth Fong, Mandela Patrick, and Andrea Vedaldi. 2019. Understanding deep networks via extremal perturbations and smooth masks. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 2950–2958. 651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

699

701

703

704

- Yash Goyal, Amir Feder, Uri Shalit, and Been Kim. 2019. Explaining classifiers with causal concept effect (cace). *arXiv preprint arXiv:1907.07165*.
- David Harbecke and Christoph Alt. 2020. Considering likelihood in NLP classification explanations with occlusion and language modeling. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics: Student Research Workshop*, pages 111–117, Online. Association for Computational Linguistics.
- Peter Hase, Harry Xie, and Mohit Bansal. 2021. The out-of-distribution problem in explainability and search methods for feature importance explanations. *Advances in Neural Information Processing Systems*, 34.
- Sara Hooker, Dumitru Erhan, Pieter-Jan Kindermans, and Been Kim. 2019. A benchmark for interpretability methods in deep neural networks. In *Advances in Neural Information Processing Systems*, volume 32. Curran Associates, Inc.
- Huggingface. 2020. Pretrained models transformers 3.3.0 documentation. https: //huggingface.co/transformers/ pretrained\_models.html. (Accessed on 09/30/2020).
- Xisen Jin, Zhongyu Wei, Junyi Du, Xiangyang Xue, and Xiang Ren. 2020. Towards hierarchical importance attribution: Explaining compositional semantics for neural sequence models. In *International Conference on Learning Representations*.
- Daniel Khashabi, Snigdha Chaturvedi, Michael Roth, Shyam Upadhyay, and Dan Roth. 2018. Looking beyond the surface: A challenge set for reading comprehension over multiple sentences. 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 252–262, New Orleans, Louisiana. Association for Computational Linguistics.
- Siwon Kim, Jihun Yi, Eunji Kim, and Sungroh Yoon. 2020. Interpretation of NLP models through input marginalization. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 3154–3167, Online. Association for Computational Linguistics.
- Diederik P Kingma and Jimmy Ba. 2015. Adam: A method for stochastic optimization. *Published as a conference paper at the 3rd International Conference for Learning Representations, San Diego.*

Vivian Lai and Chenhao Tan. 2019. On human predictions with explanations and predictions of machine learning models: A case study on deception detection. In *Proceedings of the conference on fairness, accountability, and transparency*, pages 29–38.

705

706

710

711

712

713 714

715

716

717

718

719

720

721

722

723 724

725

726

727

728

729

730

731

733 734

736

737

741

742

743

744

745 746

747

748

750

751

755

- Jiwei Li, Will Monroe, and Dan Jurafsky. 2016. Understanding neural networks through representation erasure. *arXiv preprint arXiv:1612.08220*.
- Frederick Liu and Besim Avci. 2019. Incorporating priors with feature attribution on text classification. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 6274–6283, Florence, Italy. Association for Computational Linguistics.
- Scott M Lundberg and Su-In Lee. 2017. A unified approach to interpreting model predictions. In Advances in neural information processing systems, pages 4765–4774.
- Judea Pearl. 2009. *Causality*. Cambridge university press.
- Ribeiro. 2021. marcotcr/lime: Lime: Explaining the predictions of any machine learning classifier. https://github.com/marcotcr/ lime. (Accessed on 05/17/2021).
- Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. Why should i trust you?: Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, pages 1135– 1144. ACM.
- Marko Robnik-Šikonja and Igor Kononenko. 2008. Explaining classifications for individual instances. *IEEE Transactions on Knowledge and Data Engineering*, 20(5):589–600.
- Cynthia Rudin. 2019. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5):206–215.
- Richard Socher, Alex Perelygin, Jean Wu, Jason Chuang, Christopher D Manning, Andrew Y Ng, and Christopher Potts. 2013. 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.
- Sarah Wiegreffe and Ana Marasović. 2021. Teach me to explain: A review of datasets for explainable nlp. *arXiv preprint arXiv:2102.12060.*
- Matthew D Zeiler and Rob Fergus. 2014. Visualizing and understanding convolutional networks. In *European conference on computer vision*, pages 818–833. Springer.

Yujia Zhang, Kuangyan Song, Yiming Sun, Sarah Tan, and Madeleine Udell. 2019. " why should you trust my explanation?" understanding uncertainty in lime explanations. *arXiv preprint arXiv:1904.12991*. 757

758

759

760

761

762

763

764

765

Bolei Zhou, Aditya Khosla, Agata Lapedriza, Aude Oliva, and Antonio Torralba. 2016. Learning deep features for discriminative localization. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2921–2929.

# **Appendix for:**

# Double Trouble: How to *not* explain a text classifier's decisions using counterfactuals synthesized by masked language models?

# A IM explanations have smaller attribution magnitude per token and lower word coverage

To further understand the impact of the fact that BERT tends to not change a to-remove token (Sec. 7.2), here, we quantify the magnitude of attribution given by IM and its coverage of important words in an example.

**Smaller attribution magnitude** Across three datasets, the average absolute values of attribution scores (which are  $\in [-1, 1]$ ) of IM are not higher than that of LOO<sub>empty</sub> (Table A1). Especially in MultiRC, IM average attribution magnitude is  $4.5 \times$  lower than that of LOO<sub>empty</sub> (0.02 vs 0.09).

**Lower word coverage** We define *coverage* as the average number of highlighted tokens per example (e.g. Fig. 1) after binarizing a heatmap at the method's optimal threshold.

The coverage of  $LOO_{empty}$  is much higher than that of IM on SST (40% vs 30%) and MultiRC examples (27% vs 6%), which is consistent with the higher *recall* of  $LOO_{empty}$  (Table A2; a vs. b). For e-SNLI, although IM has higher coverage than  $LOO_{empty}$  (14% vs. 10%), the coverage of  $LOO_{empty}$  is closer to the human coverage (9%). That is, IM assigns high attribution incorrectly to many words, resulting in a substantially lower *precision* than  $LOO_{empty}$ , according to e-SNLI L3 annotations (Table 3b; 0.3814 vs. 0.4687).

In sum, chaining our results together, we found BERT to often replace a token $x_i$ by an exact-match
with a high likelihood (Sec. 7.2), which sets a low empirical upper-bound on attribution values of IM,
causing IM explanations to have smaller attribution magnitude. As the result, after binarization, fewer
tokens remain highlighted in IM binary maps (e.g. Fig. 3).

Method	SST	e-SNLI	MultiRC
$LOO_{empty}$	$\textbf{0.22} \pm 0.27$	$0.15\pm0.24$	$\textbf{0.09} \pm 0.09$
IM	$0.17\pm0.27$	$0.15\pm0.27$	$0.02\pm0.09$

Table A1: The average absolute value of attribution scores per token of  $LOO_{empty}$  is consistently higher than that of IM.

Explanations	SST	e-S	NLI	MultiRC
generated by		L2	L3	
(a) LOO <sub>empty</sub>	40%	19%	10%	27%
(b) IM	30%	21%	14%	6%
(c) Human	37%	18%	9%	16%
# tokens per example	20	2	4	299

Table A2: Compared to IM, the coverage of LOO<sub>empty</sub> is closer to the coverage of human explanations.

SS	ST example. Groundtruth: "positive"								
S	may not	have ge	enerated many	sparks ,	but with his a	ffection for Astoria and its people he has given his tale a warm glow.			
$S_1$	may not	have ge	enerated many	sparks,	but with his a	ffection for Astoria and its people he has given his tale a warm glow .			
	0.9494	he	0.9105	given	0.9632	a			
	0.0103	it	0.0285	lent	0.0270	its			
	0.0066	,	0.0143	gave	0.0033	another			

Figure A1: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the SST "positive" example. In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

SS	ST exampl	e. Ground	dtruth: "neg	gative"		
S	Villeneuv	e spends /	too <mark>much</mark> ti	ime <mark>wallo</mark>	wing <mark>in</mark> Bib	bi 's generic angst ( there are a lot of shots of her gazing out windows ).
$S_1$	Villeneuv	ve spends t	too much t	ime wallo	owing in Bil	Bibi 's generic angst ( there are a lot of shots of her gazing out windows ).
	0.9987	much	0.9976	time	0.9675	in
	0.0011	little	0.0005	money	0.0066	with
	0.0001	some	0.0003	space	0.0062	on

Figure A2: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the SST "negative" example. In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

e-s	e-SNLI example. Groundtruth: "entailment"								
P	The two	<mark>farmers</mark> a	ure workin	ig on a piece of	f <mark>John</mark> I	Deere	equipment .		
Η	John De	ere equip	ment is be	ing worked on	by <mark>two</mark>	<mark>farme</mark>	ers		
$P_1$	The two	The two farmers are working on a piece of John Deere equipment							
$H_1$	John De	eere equip	ment is be	eing worked or	ı by two	o farm	ers		
	0.9995	john	0.9877	equipment	0.971	1 jo	hn		
	0.0000	johnny	0.0057	machinery	0.024	3 th	e		
	0.0000	henry	0.0024	hardware	0.000	5 a			

Figure A3: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the e-SNLI "entailment" example which contains a pair of premise (P) and hypothesis (H). In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

e-S	SNLI exa	mple. Grou	undtruth: '	'neutra	l"	
Р	A man u	ses a projec	tor to give	e a pres	entation .	
Η	A man is	giving a p	resentation	1 in <mark>fro</mark>	nt <mark>of a lar</mark>	<mark>ge</mark> crowd .
		ses a projec				
$H_1$	A man is	giving a p	resentation	1 in fro	nt of a la	rge crowd .
	1.0000	front	0.9999	of	0.9993	a
	0.0000	view	0.0000	to	0.0005	the
	0.0000	presence	0.0000	with	0.0001	another

Figure A4: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the e-SNLI "neutral" example which contains a pair of premise (P) and hypothesis (H). In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

1710		imple. Grou		realement	1100 (00					
Р						force . Any time an object changes motion , a force has been				
	applied . In what ways can this happen ? Force can cause an object at rest to start moving . Forces can cause objects to									
	speed up or slow down. Forces can cause a moving object to stop. Forces can also cause a change in direc-									
						moving object may change its speed, its direction, or both.				
	We know	that changes	s in motio	n require a	force . W	e know that the size of the force determines the change in				
	motion .	How much a	n objects r	notion char	nges when	a force is applied depends on two things. It depends on the				
	strength o	f the force . I	t also depe	nds on the	objects mas	s. Think about some simple tasks you may regularly do . You				
		up a baseball								
Q	• •	ors cause cha			-					
-			<u> </u>							
Α	The object	t's speed, di	rection, o	r both spee	d and direc	tion				
P1	What causes a change in motion ? The application of a force . Any time an object changes motion , a force has been applied . In what ways can this happen ? Force can cause an object at rest to start moving . Forces can cause objects to speed up or slow down . Forces can cause a moving object to stop . Forces can also cause a change in direction . In short , forces cause changes in motion . The moving object may change its speed , its direction , or both . We know that changes in motion require a force . We know that the size of the force determines the change in motion . How much an objects motion changes when a force is applied depends on two things . It depends on the strength of the force . It also depends on the objects mass . Think about some simple tasks you may regularly do . You may pick up a baseball . This requires only a very small force .									
	0.9927	moving	0.9891	change	0.9995	or				
	0.0023	moved	0.0033	alter	0.0004	and				
	0.0016	stationary	0.0018	affect	0.0000	etc				
$Q_1$	John Deer	re equipment	is being w	orked on b	y two farm	ers				
$A_1$										

Figure A5: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the MultiRC "True" example which contains a triplet of paragraph (P), question (Q) and answer (A). In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

M	MultiRC example. Groundtruth & Prediction: "False" (confidence: 0.74)								
Р						ved in Earths past . Only a tiny number of them became fos-			
						sils . Fossils are our best clues about the history of life on Earth.			
						They tell us that life on Earth has changed over time. Fossils in			
						e living today. Fossils in older rocks are less like living organisms.			
				•		d. Was it land or marine ? Fossils can even tell us if the water was			
		<b>1</b>		<b>1</b>		to ancient climates .			
Q					rom fossils	?			
А	Who live	ed in preh	istoric time	es					
P <sub>1</sub>	Thora he	wa haan i	nonu organ	isms that	have lived	l in Earths past. Only a tiny number of them became fossils. Still			
<b>F</b> 1						our best clues about the history of life on Earth . Fossils provide			
						fe on Earth has changed over time. Fossils in younger rocks look			
						sils in older rocks are less like living organisms . Fossils can tell us			
						marine ? Fossils can even tell us if the water was shallow or deep .			
	Fossils c	an even p	rovide clue	es to ancie	ent climates	3			
	0.9984	life	0.9982	earth	0.9980	time			
	0.0004	living	0.0007	mars	0.0007	millennia			
	0.0002	things	0.0002	land	0.0003	history			
$Q_1$	What are	e three thi	ngs scienti	sts learn f	rom fossils	9 ?			
$A_1$	Who lived in prehistoric times								

Figure A6: BERT often correctly predicts the masked tokens (denoted in red, green, blue rectangles) and assigns a high likelihood to the tokens that are labeled important by humans in the MultiRC "False" example which contains a triplet of paragraph (P), question (Q) and answer (A). In each panel, we show the top-3 tokens suggested by BERT and their associated likelihoods.

SST	SST example. Groundtruth & Prediction: "negative" (confidence: 1.00)								
S	For starters, the story is just too slim.								
SIM	For <mark>starters</mark> , the <mark>story</mark> is just too slim .								
	IoU: 0.33, precision: 0.50, recall: 0.50								
$S_{\text{LOO}}$	For starters, the story is just too slim.								
	IoU: 0.75, precision: 1.00, recall: 0.75								

Figure A7: The set of explanatory words given by  $LOO_{empty}$  covers 75% of human highlights with higher precision and IoU in the SST "negative" example while there are a half of tokens given by IM are in correlation with human explanations.

e-SN	LI example. Groundtruth & Prediction: "contradiction" (confidence: 1.00)
Р	Two men are cooking food together on the corner of the street.
Η	The two men are running in a race.
<b>_</b>	
PIM	Two men are cooking food together on the corner of the street .
H <sub>IM</sub>	The two men are running in a race.
	IoU: 0.25, precision: 0.33, recall: 0.50
	Two men are cooking food together on the corner of the street.
H <sub>LOO</sub>	The two men are running in a race.
	IoU: 0.50, precision: 0.50, recall: 1.00

Figure A8: The set of explanatory words given by  $LOO_{empty}$  covers **all** highlights (higher precision and IoU) that are important to human in the e-SNLI "contradiction" example which contains a pair of premise (P) and hypothesis (H) while there are **a half** of tokens given by IM are in correlation with human explanations.

e-SN	LI example. Groundtruth & Prediction: "neutral" (confidence: 1.00)
Р	Woman in a dress standing in front of a line of a clothing line , with clothes hanging on the line .
Н	Her dress is <mark>dark</mark> blue .
P <sub>IM</sub>	Woman in a dress standing in front of a line of a clothing line, with clothes hanging on the line.
H <sub>IM</sub>	Her dress is dark blue .
	IoU: 0.00, precision: 0.00, recall: 0.00
PLOO	Woman in a dress standing in front of a line of a clothing line, with clothes hanging on the line.
H <sub>LOO</sub>	Her dress is dark blue.
	IoU: 0.33, precision: 0.33, recall: 1.00

Figure A9: The set of explanatory words given by LOO<sub>empty</sub> covers **all** highlights (higher precision and IoU) that are important to human in the e-SNLI "neutral" example which contains a pair of premise (P) and hypothesis (H) while there are **none** tokens given by IM are in correlation with human explanations.

Mulf	<b>iRC</b> example. Groundtruth & Prediction: "True" (confidence: 0.90)
P	There have been many organisms that have lived in Earths past. Only a tiny number of them became fossils. Still, scientists learn a lot from fossils. Fossils are our best clues about the history of life on Earth. Fossils provide evidence about life on Earth. They tell us that life on Earth has changed over time. Fossils in younger rocks look like animals and plants that are living today. Fossils in older rocks are less like living organisms. Fossils can tell us about where the organism lived. Was it land or marine? Fossils can even tell us if the water was shallow or deep. Fossils can even provide clues to ancient climates.
Q	What happened to some organisms that lived in Earth 's past ?
Α	They became fossils . Others did not become fossils
P <sub>IM</sub>	There have been many organisms that have lived in <b>Earths</b> past. Only a tiny number of them became fossils. Still, scientists learn a lot from fossils. Fossils are our best clues about the history of life on Earth. Fossils provide evidence about life on Earth. They tell us that life on Earth has changed over time. Fossils in younger rocks look like animals and plants that are living today. Fossils in older rocks are less like living organisms. Fossils can tell us about where the organism lived. Was it land or marine? Fossils can even tell us if the water was shallow or deep. Fossils can even provide clues to ancient climates.
QIM	What happened to some organisms that lived in Earth 's past?
A <sub>IM</sub>	They became fossils . Others did not become fossils
	IoU: 0.16, precision: 0.50, recall: 0.19
P <sub>LOO</sub>	There have been many organisms that have lived in Earths past Only a tiny number of them became fossils. Still, scientists learn a lot from fossils. Fossils are our best clues about the history of life on Earth. Fossils provide evidence about life on Earth. They tell us that life on Earth has changed over time. Fossils in younger rocks look like animals and plants that are living today. Fossils in older rocks are less like living organisms. Fossils can tell us about where the organism lived. Was it land or marine? Fossils can even tell us if the water was shallow or deep. Fossils can even provide clues to ancient climates
	What happened to some organisms that lived in Earth 's past?
ALOO	They became fossils . Others did not become fossils
	IoU: 0.56, precision: 0.57, recall: 0.95

Figure A10: The set of explanatory words given by LOO<sub>empty</sub> covers 95% of human highlights with higher precision and IoU in the MultiRC "True" example which contains a triplet of paragraph (P), question (Q) and answer (A) while there are only few tokens given by IM are in correlation with human explanations.

Mult	iRC example. Groundtruth & Prediction: "False" (confidence: 0.99)									
Р	There have been many organisms that have lived in Earths past . Only a tiny number of them became fossils . Still									
	, scientists learn a lot from fossils . Fossils are our best clues about the history of life on Earth . Fossils provide									
	evidence about life on Earth . They tell us that life on Earth has changed over time . Fossils in younger rocks look									
	like animals and plants that are living today. Fossils in older rocks are less like living organisms. Fossils can tell									
	us about where the organism lived . Was it land or marine ? Fossils can even tell us if the water was shallow or deep . Fossils can even provide clues to ancient climates .									
	-									
Q	What is a major difference between younger fossils and older fossils ?									
A	Older rocks are rougher and thicker than younger fossils									
P <sub>IM</sub>	There have been many organisms that have lived in Earths past . Only a tiny number of them became fossils . Still , scientists learn a lot from fossils . Fossils are our best clues about the history of life on Earth . Fossils provide evidence about life on Earth . They tell us that life on Earth has changed over time . Fossils in younger rocks look like animals and plants that are living today . Fossils in older rocks are less like living organisms . Fossils can tell us about									
	where the organism lived . Was it land or marine ? Fossils can even tell us if the water was shallow or deep . Fossils can even provide clues to ancient climates .									
Q <sub>IM</sub>	What is a major difference between younger fossils and older fossils ?									
A <sub>IM</sub>	Older rocks are rougher and thicker than younger fossils									
	IoU: 0.06, precision: 0.18, recall: 0.08									
P <sub>LOO</sub>	There have been many organisms that have lived in Earths past. Only a tiny number of them became fossils. Still									
	, scientists learn a lot from fossils . Fossils are our best clues about the history of life on Earth . Fossils provide									
	evidence about life on Earth . They tell us that life on Earth has changed over time . Fossils in younger rocks look									
	like animals and plants that are living today. Fossils in older rocks are less like living organisms. Fossils can tell									
	us about where the organism lived . Was it land or marine ? Fossils can even tell us if the water was shallow or deep									
	. Fossils can even provide clues to ancient climates.									
QLOO	What is a major difference between younger fossils and older fossils ?									
ALOO	Older rocks are rougher and thicker than younger fossils									
	IoU: 0.22, precision: 0.25, recall: 0.67									

Figure A11: The set of explanatory words given by  $LOO_{empty}$  covers two thirds of human highlights with higher precision and IoU in the MultiRC "False" example which contains a triplet of paragraph (P), question (Q) and answer (A) while there are two tokens given by IM are in correlation with human explanations.

SST example. Groundtruth & Prediction: "positive"		
S	Enormously entertaining for moviegoers of any age.	
$S_1$	Enormously entertaining for moviegoers of any age .	
$S_2$	Enormously <b>entertaining</b> for moviegoers of any age .	
<b>S</b> <sub>3</sub>	Enormously entertaining for moviegoers of any age .	
$S_4$	Enormously entertaining for moviegoers of any age .	
$S_5$	Enormously entertaining for moviegoers of any age.	
$S_6$	Enormously entertaining for moviegoers of <b>any</b> age .	
<b>S</b> <sub>7</sub>	Enormously entertaining for moviegoers of any age.	

Figure A12: When a word is **removed**, the predicted labels of all resulting sentences ( $S_1$  to  $S_7$ ) are still "positive" with a confidence score of 1.0.

e-SNLI example. Groundtruth: "entailment"		
Р	Two women having drinks and smoking cigarettes at the bar.	entailment
Η	Two women are at a bar .	(0.99)
P <sub>1</sub>	<b>Two</b> women having drinks and smoking cigarettes at the bar.	entailment
H <sub>1</sub>	Two women are at a bar .	(0.98)
<b>P</b> <sub>2</sub>	Two women having drinks and smoking cigarettes at the bar.	neutral
$H_2$	Two women are at a bar.	(0.93)
<b>P</b> <sub>3</sub>	Two women having drinks and smoking cigarettes at the bar .	entailment
H <sub>3</sub>	Two women are at a bar .	(0.99)
$\mathbf{P}_4$	Two women having <b>drinks</b> and smoking cigarettes at the bar .	entailment
H <sub>5</sub>	Two women are at a bar .	(0.99)
<b>P</b> 5	Two women having drinks <b>and</b> smoking cigarettes at the bar .	entailment
$H_5$	Two women are at a bar .	(0.99)
P <sub>6</sub>	Two women having drinks and <b>smoking</b> cigarettes at the bar .	entailment
H <sub>6</sub>	Two women are at a bar .	(0.99)
<b>P</b> <sub>7</sub>	Two women having drinks and smoking <b>cigarettes</b> at the bar .	entailment
H <sub>7</sub>	Two women are at a bar .	(0.99)
<b>P</b> <sub>8</sub>	Two women having drinks and smoking cigarettes <b>at</b> the bar .	entailment
$H_8$	Two women are at a bar .	(0.98)
<b>P</b> 9	Two women having drinks and smoking cigarettes at <b>the</b> bar .	entailment
H9	Two women are at a bar .	(0.98)
$P_{10} \\$	Two women having drinks and smoking cigarettes at the <b>bar</b> .	entailment
$H_{10}$	Two women are at a bar .	(0.97)
P <sub>11</sub>	Two women having drinks and smoking cigarettes at the bar -	entailment
$H_{11}$	Two women are at a bar .	(0.99)
P <sub>12</sub>	Two women having drinks and smoking cigarettes at the bar .	entailment
H <sub>12</sub>		(0.99)
P <sub>13</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
H <sub>13</sub>	Two women are at a bar .	(0.98)
P <sub>14</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
$H_{14}$	Two women <b>are</b> at a bar .	(0.99)
P <sub>15</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
$H_{15}$	Two women are <b>at</b> a bar.	( <b>0.84</b> )
P <sub>16</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
$H_{16}$	Two women are at <b>a</b> bar.	(0.97)
P <sub>17</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
$H_{17}$	Two women are at a <b>bar</b> .	(0.54)
P <sub>18</sub>	Two women having drinks and smoking cigarettes at the bar.	entailment
$H_{18}$	Two women are at a bar -	(0.95)

Figure A13: The removal of each token in both premise and hypothesis in e-SNLI example which contains a pair of premise (P) and hypothesis (H) **infrequently change the prediction**. Specifically, only the example of  $(P_2, H_2)$  shifted its prediction to "neutral" while the remaining partially-removed examples do not change their original prediction with high confidence score in parentheses.