Analysing the Robustness of Dual Encoders for Dense Retrieval Against Misspellings

Sidiropoulos, G.; Kanoulas, E.

DOI
10.1145/3477495.3531818

Publication date
2022

Document Version
Final published version

Published in
SIGIR ’22

License
Article 25fa Dutch Copyright Act (https://www.openaccess.nl/en/in-the-netherlands/you-share-we-take-care)

Citation for published version (APA):
Analyzing the Robustness of Dual Encoders for Dense Retrieval Against Misspellings

Georgios Sidiropoulos
University of Amsterdam
Amsterdam, The Netherlands
g.sidiropoulos@uva.nl

Evangelos Kanoulas
University of Amsterdam
Amsterdam, The Netherlands
e.kanoulas@uva.nl

ABSTRACT

Dense retrieval is one of the standard approaches for document and passage ranking. The dual-encoder architecture is widely adopted for scoring question-passage pairs due to its efficiency and high performance. Typically, dense retrieval models are evaluated on clean and curated datasets. However, when deployed in real-life applications, these models encounter noisy user-generated text. That said, the performance of state-of-the-art dense retrievers can substantially deteriorate when exposed to noisy text. In this work, we study the robustness of dense retrievers against typos in the user question. We observe a significant drop in the performance of the dual-encoder model when encountering typos and explore ways to improve its robustness by combining data augmentation with contrastive learning. Our experiments on two large-scale passage ranking and open-domain question answering datasets show that our proposed approach outperforms competing approaches. Additionally, we perform a thorough analysis on robustness. Finally, we provide insights on how different typos affect the robustness of embeddings differently and how our method alleviates the effect of some typos but not of others.

CCS CONCEPTS

• Information systems → Retrieval models and ranking.

KEYWORDS

dense retrieval; dual-encoder; robustness; typos; misspellings

ACM Reference Format:

1 INTRODUCTION

With the advances in neural language modeling [3], learning dense representations for text has become a vital component in many information retrieval (IR) tasks. In passage ranking and open-domain question answering, dense retrieval has become a new paradigm to retrieve relevant passages [6, 7, 9]. In contrast to traditional term-based IR models (TF-IDF and BM25) that fail to capture beyond lexical matching, dense retrieval learns dense representations of questions and passages for semantic matching.

A typical approach for dense retrieval involves learning a dual-encoder for embedding the questions and passages [6]. A dual-encoder model consists of two separate neural networks optimized to score relevant (i.e., positive) question-passage pairs higher than irrelevant (i.e., negative) ones. At inference time, the score of a question-passage pair is computed as the inner product of the corresponding question and passage embeddings. Due to their high efficiency, dual-encoders are popular first-stage rankers in large-scale settings (in contrast to cross-encoders where even though they can achieve higher performance, they are not indexable and therefore are used as re-rankers [4, 15]). The whole corpus can be encoded and indexed offline, while at inference time, high-scoring passages with respect to a question can be found using efficient maximum inner product search [5].

So far, dense retrieval models have been evaluated on clean and curated datasets. However, these models will encounter user-generated noisy questions when deployed in real-life applications. Questions can include typos because of users mistyping words, such as keyboard typos (additional/missing character and character substitution), phonetic typing errors due to the close pronunciation, and misspellings. How these typos affect the encoding of questions and whether dense dual-encoder retrieval models are robust to them is not studied yet.

Works on text classification have shown that deep neural language models such as BERT are not robust against typos [13, 16], even though they apply the WordPiece tokenization. Ma et al. [10] and Zhuang et al. [17] showed that typos can confuse even advanced BERT-based cross-encoders for re-ranking [2, 4, 12] and proposed data augmentation training for building typo-robust re-rankers. Additionally, Ma et al. [10] showed that bringing closer in the latent space the representations of the positive question-passage pairs of different questions while being far apart from negative ones can increase robustness.

While the aforementioned works studied robustness for the case of re-ranking, improving the robustness of dense retrieval for first-stage ranking has not been explored in-depth yet. Intuitively, if typos cause an inferior first-stage ranking, that will already negatively affect the performance of the re-ranker. Therefore, robustness for first-stage ranking is crucial for the overall performance. To the best of our knowledge, Zhuang et al. [17] is the only work that studied the first-stage ranking and used data augmentation to improve the robustness of a BERT-based Siamese encoder.
In this paper, we study in-depth the robustness of dense retrieval for the case of dual-encoder architecture. We propose an approach that combines data augmentation with contrastive learning for robustifying dual-encoders against questions with typos. In detail, alongside augmenting questions with typos, we propose to use a contrastive loss that brings the representation of a question close to its typoed variations in the latent space while keeping it distant from other distinct questions.

We aim to answer the following research questions:

**RQ1** Can data augmentation, contrastive learning, and their combination improve the robustness of dense retrieval to typos?

**RQ2** Do certain typoed words affect the robustness of the question encoding more than others?

**RQ3** Do the proposed method improve the robustness of the question encoding by ways other than simply learning to ignore the typoed word?

Our main contributions are the following: (i) we propose an approach for robustifying dense retrievers towards typos in user questions that combines data augmentation with contrastive learning and performs better than applying each component separately, (ii) we perform a thorough analysis on the robustness of dense retrieval, and (iii) show that typos in various words influence performance differently.

## 2 EXPERIMENTAL SETUP

In this section, we discuss the datasets, the metrics, and the robustness methods we experiment with to answer our research questions.

### 2.1 Datasets

We conduct our experiments on two large-scale datasets, namely, MS MARCO passage ranking [11], and Natural Questions [8]. In MS MARCO passage ranking, the goal is to rank passages based on their relevance to a question (i.e., the probability of including the answer). The data collection consists of 8.8 million passages; the questions were selected from Bing search logs. Natural Questions is a large-scale dataset for open-domain QA over Wikipedia, and its questions were selected from Google search logs. Table 1 shows the statistics of the two datasets.

**Table 1: Number of questions in each dataset, and the average length of question.**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Train</th>
<th>Dev</th>
<th>Test</th>
<th>Avg. q length</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS MARCO</td>
<td>502,939</td>
<td>6,980</td>
<td>6,837</td>
<td>5.94</td>
</tr>
<tr>
<td>Natural Questions</td>
<td>79,168</td>
<td>8,757</td>
<td>3,610</td>
<td>9.20</td>
</tr>
</tbody>
</table>

### 2.2 Metrics

To measure the retrieval performance on MS MARCO, we use the official metric MRR (@(10) alongside the commonly reported Recall (R) at top-k ranks [7, 14]. Following previous work on Natural Questions, we use answer recall (AR) at the top-K retrieved passages [6, 14]. Answer recall measures whether at least one of the top-k retrieved passages contains the ground-truth answer.

## 2.3 Methods

In this section, we describe the dual-encoder model we use for our experiments. Moreover, we present the three approaches we apply as extensions to this model in order to increase robustness.

**Dense Retriever (DR)** is a dual-encoder BERT-based model used for scoring question-passage pairs [6]. Given a question \( q \), a relevant passage \( p^+ \) and a set of irrelevant passages \( \{p_1^-, p_2^-, \ldots, p_n^-\} \), the model learns to rank \( p^+ \) higher than the negative passages via the optimization of the negative log-likelihood of the relevant passage:

\[
L_1(q, p^+, p_1^-, \ldots, p_n^-) = -\log \frac{e^{\text{sim}(q, p^+)}}{\sum_{i=1}^n e^{\text{sim}(q, p_i^-)}}.
\]

**Data Augmentation (DR + Data augm.)** is one of the traditional approaches for robustifying neural models. By exposing DR on questions with and without typos, the model learns to be invariant to typos. Similar to Zhuang et al. [17], for each original correctly written question, on training time, we draw an unbiased coin. If the result is heads, we use the original question for training. If the result is tails, we use one of its typoed variations.

**Contrastive learning (DR + CL)** of representations works by maximizing the agreement between differently augmented views of the same object. We propose a contrastive loss that compares the similarity between a question and its typoed variations and other distinct questions. In contrast with data augmentation, which explicitly trains on typoed question-passage pairs, here such pairs are seen implicitly only. In detail, in addition to Equation 1, we introduce a loss that enforces that a question, \( q \) and its typoed variations \( q^\dagger \) are close together in the latent space while being far apart from other distinct questions \( \{q_1^-, q_2^-, \ldots, q_n^-\} \):

\[
L_2(q, q_1^+, q_1^-, \ldots, q_n^-) = -\log \frac{e^{\text{sim}(q, q_1^+)}}{\sum_{j=1}^n e^{\text{sim}(q, q_j^-)}}.
\]

The final loss is a weighted average of the two losses:

\[
L = w_1 \cdot L_1 + w_2 \cdot L_2.
\]

The weights \( w_1 \) and \( w_2 \) are hyper-parameters and therefore need to be defined. Giving equal weights to the two losses is an effective and straightforward combination method which we used in our experiments.

**Combination (DR + Data augm. + CL)** method consists of data augmentation combined with contrastive learning. Specifically, we propose alongside augmenting questions with typos to use the contrastive loss of Equation 2 that brings the representation of a question close to its typoed variations while keeping it distant from other distinct questions. The final loss is a weighted average of the three losses:

\[
L = w_1 \cdot L_1 + w_2 \cdot L_2 + w_3 \cdot L_3.
\]
where $\mathcal{L}_3$ represents the data augmentation and is computed similarly to Equation 1 but for the typoed variation $q^*$ of the original question $q$. For our experiments, we use an equal weighting setting for the weights $w_1, w_2$, and $w_3$.

2.4 Simulating Typos
To assess the robustness of the proposed methods, a large-scale dataset for passage retrieval with typoed questions is necessary. Unfortunately such a dataset does not exist, and therefore we build one by simulating typos over the original Natural Questions and MS MARCO datasets. In detail, we simulate typos produced by humans by augmenting the original questions in the dataset with synthetically generated typoed ones.

In order to simulate typos, we apply the following transformations that often occur in human-generated questions.

- Random: Inserts, deletes, swaps, or substitutes a random character; e.g., committee $\rightarrow \{c\text{ommittee, com\text{mitte, com\text{mitt}, com\text{mittee}}\}$.
- Keyboard: Swaps a random character with those close to each other on the QWERTY keyboard; e.g., committee $\rightarrow$ committee.
- Common misspellings: Replaces words with misspelled ones, defined in a dictionary of common user-generated misspellings; e.g., committee $\rightarrow$ commitee.

2.5 Implementation Details
The DR model used in our experiments is trained using the in-batch negative setting described in [6]. The question and passage BERT encoders are trained for 50K steps, with a batch size of 48. The learning rate is set to $2e^{-5}$ using Adam, and the rate of the linear scheduling with a warm-up is set to 0.1. Moreover, we use the same hyper-parameters for the three robustifying methods described in Section 2.3, in order to ensure a fair comparison.

For generating typos in the training phase as well as building the typo-robustness test set, we use the open-source Aug library [1]. Each word in a question gets transformed with a probability of 0.2, and the transformation type (Section 2.4) gets chosen at random.

3 RESULTS
In this section, we present our experimental results that answer our research questions. We aim to answer RQ1 by comparing the retrieval performance of the methods we consider (Section 2.3) for two settings: clean questions and questions with typos. In Table 2, we observe that on clean questions, data augmentation as well as our two proposed approaches, namely, contrastive learning and data augmentation combined with contrastive learning do not harm the performance. Moreover, all the approaches for robustifying DR are performing significantly better compared to the original DR, on questions with typos. That indicates that they successfully robustify the underlying dual-encoder model. That said, our proposed data augmentation combined with contrastive learning approach holds the best performance.

Following previous works, we randomly introduce typos to questions. However, we want to investigate if the performance of the approaches we consider remains the same irrespectively of the word in which the typo appears. To answer RQ2, we create two additional test settings for the case of questions with typos. Specifically, we create (i) a setting where typos appear only in non-stopwords, and (ii) a setting where typos appear only in utterances with lexical match with the relevant passage.\(^3\) In detail, we consider the overlapping consecutive words between the ground-truth passage and the question (e.g., “Who was the president of the united states during wwi?”, and “Woodrow Wilson, a leader of the Progressive Movement, was the 28th President of the United States (1913-1921). After a policy of neutrality at the outbreak of World War I, he led America into war,” mark the “president of the united states” as available utterance to introduce typos). The highly discriminative utterances obtained through this heuristic are typically entity mentions.

As we can see in Table 3 and by comparing the numbers with the results in Table 2, the effectiveness of the methods varies across the three settings. Particularly, robustness deteriorates when typos do not appear randomly. In detail, the most significant losses occur when typos appear on discriminative utterances. To this extent, our proposed data augmentation combined with contrastive learning approach remains the best performing one across all setting.

To better understand the discrepancy in robustness between the three settings of questions with typos, we conduct the following analysis. For the setting where typos randomly appear on questions, we study how the frequency on the training set of the typoed words at test time affects robustness. As shown in Figure 1, there is a strong connection between the frequency of the typoed words and the retrieval performance. As the frequency of the typoed words decreases, the performance drops significantly. To this extent, our proposed data augmentation combined with contrastive learning approach remains the best performing one, with the performance gap increasing as the frequency of the typoed word decreases. The results in Figure 1 can also explain why we observe the highest losses in performance on the setting with typos in discriminative utterances. In general, the discriminative utterances (entity mentions) diversity between the dataset splits is higher compared to other words appearing in questions (e.g., interrogative, linking words).

\[\text{Figure 1: Retrieval performance (Average Recall@50) w.r.t the frequency of the training set, of the typoed words at test-time, on MS MARCO (Dev). Questions are split into bins w.r.t the frequency of their typoed words.}\]

\(^3\)We build the new settings using the same probability for introducing typos (Section 2.5), and we do not retrain the models on the new settings.
Table 2: Retrieval results for the settings of (i) clean questions (Original), and (ii) questions with typos (Typos in Random Words). Statistical significance difference with paired t-test ($p < 0.05$) DR=d; DR+ Data augm.=a; DR+CL=c.

<table>
<thead>
<tr>
<th>Natural Questions (Test)</th>
<th></th>
<th>MS MARCO (Dev)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Original</td>
<td>Typos in Random Words</td>
</tr>
<tr>
<td></td>
<td>AR@5</td>
<td>AR@20</td>
</tr>
<tr>
<td>DR</td>
<td>67.31</td>
<td>78.22</td>
</tr>
<tr>
<td>DR + Data augm.</td>
<td>66.45</td>
<td>79.03</td>
</tr>
<tr>
<td>DR + CL (ours)</td>
<td>66.31</td>
<td>77.42</td>
</tr>
<tr>
<td>DR + Data augm. + CL (ours)</td>
<td>67.47</td>
<td>78.83</td>
</tr>
</tbody>
</table>

Table 3: Retrieval results for the settings of (i) questions with typos in non-stopwords (Typos in Non-stopwords), and (ii) questions with typos in highly discriminative utterances (Typos in Discriminative Utterances). Stat. sig. difference w/ paired t-test ($p < 0.05$) DR=d; DR+Data augm.=a; DR+CL=c.

<table>
<thead>
<tr>
<th>Natural Questions (Test)</th>
<th></th>
<th>MS MARCO (Dev)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Typos in Non-stopwords</td>
<td>Typos in Discriminative Utterances</td>
</tr>
<tr>
<td></td>
<td>AR@5</td>
<td>AR@20</td>
</tr>
<tr>
<td>DR</td>
<td>40.60</td>
<td>55.48</td>
</tr>
<tr>
<td>DR + Data augm.</td>
<td>56.14</td>
<td>69.94</td>
</tr>
<tr>
<td>DR + CL (ours)</td>
<td>49.47</td>
<td>64.12</td>
</tr>
<tr>
<td>DR + Data augm. + CL (ours)</td>
<td>57.78$^{dac}$</td>
<td>70.77$^{dac}$</td>
</tr>
</tbody>
</table>

For RQ3, we consider a simple baseline where the typoed words are identified and removed from the question before being fed to the original DR model. We compare our best-performing approach against the aforementioned baseline. If our proposed approach only learns to ignore words with typos, then we argue that the performance of the baseline should be competitive to ours. In many cases, removing the typoed word can be a valid approach since the importance of words in a question varies. For instance, considering the question “Where was president Lincoln born?” we see that “Lincoln” is crucial for the meaning of the question while “was” adds no information. With that in mind, we study RQ3 with respect to the relative importance of the typoed words within the question.4

Our method does not simply learn to ignore words with typos since, as we can see from Figure 2, it consistently outperforms the baseline. Furthermore, Figure 2 highlights that when the importance of typoed words is low, simply ignoring them is a highly competitive approach. On the other hand, the highlights of the importance of the typoed words increases, the effectiveness of just ignoring these words decreases dramatically, to the extent that keeping the typoed words performs better. That can be attributed to the application of the WordPiece tokenizer (by the underlying BERT model) that allows DR to recover from some typos, such as when the character n-gram splits remain intact despite the typos. For instance original robustness and typoed robustness$^d$ will be split into [robust, ###ness] and [robust, ###ness, ###d] respectively.

4We define a word’s relevant importance as the ratio of its IDF to the sum of the IDFs of every word in the question.

Figure 2: Retrieval results w.r.t the relevant importance of the typoed words; on MS MARCO (Dev). Questions are split into bins w.r.t the relevant importance their typoed words.

4 CONCLUSIONS

In this work, we provided insights on the robustness of dual-encoders to typos of user questions for dense retrieval. We proposed an approach for robustifying dual-encoders that combines data augmentation with contrastive learning. Our experimental results showed that our proposed method not only improves robustness but also performs better than separately applying data augmentation or contrastive learning. Analysis of the methods we explored showed that typos in various words do not influence performance equally. In particular, typos on words that are less frequent on the training set and more important for a question are harder to address. Our proposed technique remains the best performing one in these settings, however the performance deteriorates significantly compared
to a clean question. There is a significant question that has risen throughout our study: What could a dual-encoder actually learn to fix the problem? The WordPiece tokenizer, applied by BERT, allows models to recover from some typos. However, it would be ideal if embeddings could be learned at the character n-gram level to allow recovery from typical character substitution, deletion, etc. Furthermore, word-to-word interactions during training (e.g., through a late interaction model [7]) could also allow implicitly to learn the “correct spelling” of a typoed word during training. We leave these directions as future work.

ACKNOWLEDGMENTS

This research was supported by the NWO Innovational Research Incentives Scheme Vidi (016.Vidi.189.039), the NWO Smart Culture - Big Data / Digital Humanities (314-99-301), the H2020-EU.3.4. - SOCIETAL CHALLENGES - Smart, Green And Integrated Transport (814961). All content represents the opinion of the authors, which is not necessarily shared or endorsed by their respective employers and/or sponsors.

REFERENCES