

# Robust Task-Oriented Dialogue Generation with Contrastive Pre-training and Adversarial Filtering

Shiquan Yang<sup>1</sup>, Xinting Huang<sup>2</sup>, Jey Han Lau<sup>1</sup>, and Sarah Erfani<sup>1</sup>

<sup>1</sup>The University of Melbourne, <sup>2</sup>Tencent AI Lab

<sup>1</sup>{shiquan@student., laujh@, sarah.erfani@}unimelb.edu.au, <sup>2</sup>timxthuang@tencent.com

## Abstract

Data artifacts incentivize machine learning models to learn non-transferable generalizations by taking advantage of shortcuts in the data, and there is growing evidence that data artifacts play a role for the strong results that deep learning models achieve in recent natural language processing benchmarks. In this paper, we focus on task-oriented dialogue and investigate whether popular datasets such as MultiWOZ contain such data artifacts. We found that by only keeping frequent phrases in the training examples, state-of-the-art models perform similarly compared to the variant trained with full data, suggesting they exploit these spurious correlations to solve the task. Motivated by this, we propose a contrastive learning based framework to encourage the model to ignore these cues and focus on learning generalisable patterns. We also experiment with adversarial filtering to remove “easy” training instances so that the model would focus on learning from the “harder” instances. We conduct a number of generalization experiments — e.g., cross-domain/dataset and adversarial tests — to assess the robustness of our approach and found that it works exceptionally well. Source code of our experiments is available at: <https://github.com/shiquanyang/Robust-Dialogue>.

## 1 Introduction

Task-oriented dialogue systems aim to help human accomplish certain tasks such as restaurant reservation or navigation via natural language utterances. Recently, pre-trained language models (Hosseini-Asl et al., 2020; Peng et al., 2020; Wu et al., 2020) achieve impressive results on dialogue response generation and knowledge base (KB) reasoning, two core components of dialogue systems. However, neural networks are found to be prone to learning *data artifacts* (McCoy et al., 2019; Ilyas et al., 2019), i.e. superficial statistical patterns in the training data, and as such these results may not

generalise to more challenging test cases, e.g., test data that is drawn from a different distribution to the training data.

This issue has been documented in several natural language processing (NLP) tasks (Branco et al., 2021; McCoy et al., 2019; Niven and Kao, 2019). For example, in natural language inference (NLI), where the task is to determine whether one given sentence entails the other, the models trained on NLI benchmark datasets are highly likely to assign a “contradiction” label if there exists a word *not* in the input sentences even if the true relation is “entailment”, as *not* often co-occurs with the label “contradiction” in the training set. Similar issues have also been observed in many other tasks such as commonsense reasoning (Branco et al., 2021), visual question answering (Qi et al., 2020; Niu et al., 2021), and argument reasoning (Niven and Kao, 2019). However, it’s unclear whether such shortcuts exist in popular task-oriented dialogue datasets such as MultiWOZ (Eric et al., 2019), and whether existing dialogue models are genuinely learning the underlying task or exploiting biases<sup>1</sup> hidden in the data.

To investigate this, we start by probing whether state-of-the-art dialogue models are discovering and exploiting spurious correlations on a popular task-oriented dialogue dataset. Specifically, we measure two state-of-the-art dialogue models’ performance under two different configurations: full input (original dialogue history, e.g., *I need to find a moderately priced hotel*) and partial input (dialogue history that contains only frequent phrases, e.g., *I need to*). Preliminary experiments found that these models perform similarly under the two configurations, suggesting that these models have picked up these cues — frequent word patterns which are often not meaning bearing — to make

<sup>1</sup>We use the terms *artifacts*, *biases*, *cues* and *shortcuts* to denote the same concept and use them interchangeably throughout the paper.

predictions. This implies that these models did not learn transferable generalizations for the task, and will likely perform poorly on *out-of-distribution* test data, e.g., one that has a different distribution to the training data.

To address this, we decompose task-oriented dialogue into two tasks: delexicalized response generation and KB reasoning (prediction of the right entities in the response), and explore methods to improve model robustness for the latter. Using frequent phrases as the basis of dataset bias, we experiment with contrastive learning to encourage the model to ignore these phrases to focus on meaning-bearing words. Specifically, we pre-train our language model with a contrastive objective to encourage it to learn a similar representation for an original input (e.g., *I need to find a moderately priced hotel*) and its debiased pair (e.g., *find a moderately priced hotel*) before fine-tuning it for KB entity prediction.

Another source of bias comes from the data distribution (Branco et al., 2021). We found that the KB entity distribution in MultiWOZ can be highly skewed in certain contexts, e.g., if the dialogue context starts with *I need to*, the probability of the KB entity *Cambridge* substantially exceeds chance level, which leads to inadequate learning of entities in the tail of the distribution. Here we adapt an adversarial filtering algorithm (Sakaguchi et al., 2019) to our task, which filters “easy samples” (i.e., samples in the head of the distribution) in the training data to create a more balanced data distribution so as to encourage the model to learn from the tail of the distribution.

We conduct a systematic evaluation on the robustness of our method and four state-of-the-art task-oriented dialogue systems under various out-of-distribution settings. Experimental results demonstrate that our method substantially outperforms these benchmark systems.

To summarize, our contributions are as follows:

- We propose a novel framework for training robust task-oriented dialogue systems by decomposing response generation and entity prediction.
- We propose a two-stage contrastive learning framework to debias spurious cues in the model inputs, and adapt adversarial filtering to create a more balanced training data distribution to improve the robustness of our task-oriented dialogue system.

- We perform comprehensive experiments to validate the robustness of our method against a number of strong benchmark systems in various out-of-distribution test settings and found our method substantially outperforms its competitors.

## 2 Related Work

**Task-oriented Dialogue** Traditionally, task-oriented dialogue systems are built via pipeline-based approach where four independently designed and trained modules are connected together to generate the final system responses. These include natural language understanding (Chen et al., 2016), dialogue state tracking (Wu et al., 2019a; Zhong et al., 2018), policy learning (Peng et al., 2018), and natural language generation (Chen et al., 2019). However, the pipeline-based approach can be very costly and time-consuming as each module needs module-specific training data and can not be optimized in a unified way. To address this, many end-to-end approaches (Bordes et al., 2017; Lei et al., 2018; Madotto et al., 2018) have been proposed to reduce human efforts in recent years. Lei et al. (2018) propose a two-stage sequence-to-sequence model to incorporate dialogue state tracking and response generation jointly in a single sequence-to-sequence architecture. Zhang et al. (2020) propose a domain-aware multi-decoder network to combine belief state tracking, action prediction and response generation in a single neural architecture. More recently, the field has shifted towards using large-scale pre-trained language models such as BERT (Devlin et al., 2019) and GPT-2 (Radford et al., 2019) for task-oriented dialogue modeling due to their success on many NLP tasks (Wolf et al., 2019; Zhang et al., 2019; Peng et al., 2020). Peng et al. (2020) and Hosseini-Asl et al. (2020) employed a GPT-2 based model jointly trained for belief state prediction and response generation in a multi-task fashion. Wu et al. (2020) pre-train BERT on multiple task-oriented dialogue datasets for response selection.

**Spurious Cues in NLP Dataset** Deep neural networks have achieved tremendous progress on many NLP tasks (Huang et al., 2019; Ghazvininejad et al., 2018; Xing et al., 2018; Veličković et al., 2017; Wu et al., 2016) with the emergence of large language models like BERT (Devlin et al., 2018) and GPT-2 (Radford et al., 2019). However, many recent NLP studies (Branco et al., 2021; McCoy et al., 2019; Niven and Kao, 2019; Ilyas et al., 2019; Hendrycks

et al., 2021) have found that deep neural networks are prone to exploit spurious artifacts present in the data rather than learning the underlying task. In natural language inference (NLI), (Belinkov et al., 2019) found that certain linguistic phenomenon in the NLI benchmark datasets correlate well with certain classes. For example, by only looking at the hypothesis, simple classifier models can perform as well as the model using full inputs (both hypothesis and premise). (Niven and Kao, 2019) found that BERT achieves a performance close to human on Argument Reasoning Comprehension Task (ARCT) with 77% accuracy (3% below human performance). However, they discover that the impressive performance is attributed to the exploitation of shortcuts in the dataset. (Geva et al., 2019) analyze annotator bias on NLP datasets and found that a model that uses only annotator identifiers can achieve a similar performance to one that uses the full data. In commonsense reasoning, (Branco et al., 2021) has performed a systematic investigation over four commonsense related tasks and found that most datasets experimented with are problematic with models are prone to leveraging the non-robust features in the inputs to make decisions and do not generalize well to the overall tasks intended to be conveyed by the commonsense reasoning tasks and datasets. Inspired by these studies, our paper focus on eliminating spurious correlations in task-oriented dialogue systems.

### 3 Model Architecture

#### 3.1 Overview

We decompose the dialogue generation task into two sub-tasks: delexicalized response generation and entity prediction. The delexicalized response is the response where KB entities are substituted by placeholders to reduce the complexity of the problem through a smaller vocabulary. For example, in Figure 1, *Davinci Pizzeria* is replaced by “[restaurant\_name]” in the response. We follow the delexicalization process proposed in (Hosseini-Asl et al., 2020). We employ the two-phase design because it disentangles the entity prediction task from response generation task, allowing us to focus on bias reduction for entity prediction. Our framework uses a pre-trained autoregressive model (GPT-2) as the response generator and a pre-trained bidirectional encoder (BERT) as the entity predictor. Note that GPT-2 is fine-tuned to generate the delexicalized responses while the BERT model is fine-tuned

to predict entities at every timestep during decoding, and the final response is created by replacing the placeholder tokens (generated by GPT-2) using the predicted entities (by BERT). Figure 1 presents the overall architecture. We first describe how the delexicalized response generation operates in Section 3.2 followed by entity prediction in Section 3.3. We introduce our debiasing techniques for the entity prediction model in Section 4.

#### 3.2 Delexicalized Response Generation

We follow (Hosseini-Asl et al., 2020) and fine-tune GPT-2 to generate the delexicalized responses. Note that the input is always prefixed with the dialogue history and GPT-2 is fine-tuned via cross-entropy loss to predict the next (single turn) response.<sup>2</sup>

#### 3.3 Entity Prediction

The entity prediction task can be formulated as a multi-class classification problem. The goal of the entity prediction module is to predict the correct KB entities at each timestep during the response generation process, given the dialogue context and the generated word tokens before current timestep. Formally, let  $D = [x_1, x_2, \dots, x_n]$  be the dialogue history,  $Y = [y_1, y_2, \dots, y_m]$  be the ground truth delexicalized response, where  $n$  is the number of tokens in the dialogue history,  $m$  the number of tokens in the response. During training, we fine-tune BERT to predict the entity at the  $t$ -th timestep, by taking the dialogue history and the generated tokens, i.e.,  $\bar{D} = [x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_{t-1}]$ , as the input:

$$\begin{aligned} H &= BERT_{enc}(\phi^{emb}(\bar{D})) \\ z &= g(H_{CLS}) \\ P &= \text{softmax}(z) \end{aligned}$$

where  $\phi^{emb}$  is the embedding layer of BERT,  $H_{CLS}$  the hidden state of the [CLS] token,  $g$  a linear layer, and  $P$  the probability distribution over the KB entity set. Note that the KB entity set consists of all KB entities and a special label [NULL], which is used when the token to be predicted at timestep  $t$  is not an entity (i.e., normal words). During inference, we use the delexicalized response

<sup>2</sup>To inform the model about user utterances and system utterances in the dialogue context, we add special tokens  $\langle |user| \rangle$  and  $\langle |system| \rangle$  at the beginning and end of user and system utterances for each turn of the dialogue history, following (Hosseini-Asl et al., 2020). We also add a symbol  $\langle |response| \rangle$  at the end of the dialogue history to indicate the start of the response generation.

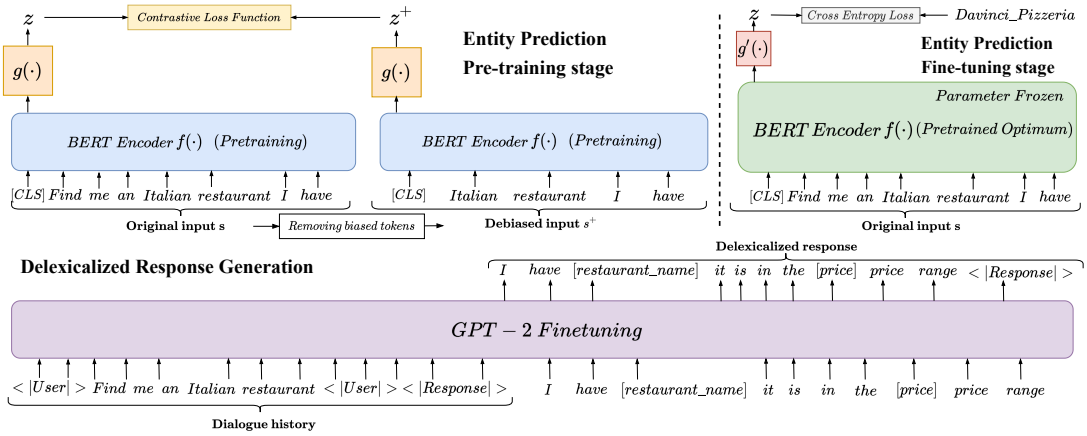


Figure 1: Overview of our proposed approach. The top shows the two-stage design for entity prediction: BERT pre-training using contrastive loss and fine-tuning using cross-entropy loss. The bottom shows the delexicalized response generation by fine-tuning GPT-2.

generated by GPT-2 as input, and at each time step select the entity with the largest probability produced by BERT as the output.

The delexicalized response generator (GPT-2) and entity predictor (BERT) are trained separately, and at test time we first generate the delexicalized response and then use it as input to the entity predictor to predict the entities at every time step. Once that’s done, we lexicalize the response by substituting the placeholder tokens with their corresponding entities to create the final response.

## 4 Debiased Training For Robust Entity Prediction

### 4.1 Contrastive Learning

The core idea of contrastive learning is to learn representations where positive pairs are embedded in a similar space while negative pairs are pushed apart as much as possible (Gao et al., 2021; Khosla et al., 2021; van den Oord et al., 2019). We follow the contrastive learning framework in (Gao et al., 2021) that takes a set of paired utterances  $S = \{(s_i, s_i^+)\}_{i=1}^N$  as inputs, where  $s_i$  denotes the original input and  $s_i^+$  denotes its positive counterparts (i.e., the debiased utterances). It employs in-batch negatives and cross-entropy loss for training. Formally, the inputs  $s_i$  and  $s_i^+$  are first mapped into feature representations in vector space as  $z_i$  and  $z_i^+$ . In our case we use BERT as our encoder to produce the features. The training loss  $\mathcal{L}$  for  $S$ , a minibatch with  $N$  pairs of utterances is:

$$\mathcal{L} = -\mathbb{E}_S \left[ \log \frac{e^{\text{sim}(z_i, z_i^+)/\tau}}{\sum_{j=1}^N e^{\text{sim}(z_i, z_j^+)/\tau}} \right]$$

where  $\tau$  is a temperature hyperparameter,  $\text{sim}$  the cosine similarity function. The critical issue of contrastive learning is to construct a *meaningful* positive counterpart, which in our case means capturing the semantic bearing words in the original utterance. We next describe three ideas to construct the positive pairs based on  $n$ -gram statistics.

#### 4.1.1 Criterion-1: Frequent $n$ -grams

We select the top-10%  $n$ -grams according to their frequency in the training data,<sup>3</sup> and create positive pairs containing: (1) an original input (dialogue history and response up to timestep  $t - 1$ ); and (2) filtered input where frequent  $n$ -grams are *removed*. As explained earlier in Section 4, this simple approach forces BERT to learn a similar representation between the full input (*I need to find a moderately priced hotel*) and debiased input (*find a moderately priced hotel*) by removing these  $n$ -grams directly.

#### 4.1.2 Criterion-2: Mutual Information

The previous approach does not consider the label information (i.e., the entities contained in the responses). To incorporate label information, we explore computing mutual information between  $n$ -grams and the entities. The idea is that we want to discover  $n$ -grams that produce strong correlation with entities, which means that BERT is likely to

<sup>3</sup>Recall that we perform entity prediction for every timestep in the response, and so for each response we have  $m$  training instances, where  $m$  is the number of tokens in the response.



pick them up as shortcuts for prediction. Formally:

$$I(A; B) = \sum_{A, B} p(A, B) \log \frac{p(A|B)}{p(A)}$$

where  $A$  is an  $n$ -gram and  $B$  a target entity.

We rank all pairs of  $n$ -grams and entities this way, and select the top-10% pairs and use their  $n$ -grams (ignoring the entities) as the candidate set where we remove them in the input to create the positive pairs as before. The detailed algorithm is shown in Algorithm 1 in appendix.

#### 4.1.3 Criterion-3: Jensen-Shannon Divergence

The previous approach accounts for label (entity) information, but has the limitation where it considers only the *presence* of an  $n$ -gram with a target entity. Here we extend the approach to also consider the *absence* of the  $n$ -gram, and what impacts this brings to the appearance of the target entity. To this end we compute the Jensen-Shannon divergence of two probability distributions: (1) entity distribution where an  $n$ -gram is present in the input ( $P$ ); and (2) entity distribution where an  $n$ -gram is absent in the input ( $Q$ ). The idea is that an  $n$ -gram is highly informative (in terms of predicting the entities) if the divergence of the distributions is high, and we want to remove these  $n$ -grams from the input. Formally:

$$JSD(P; Q) = \frac{1}{2} \sum_{x \in \mathbb{X}} P(x) \log \frac{P(x)}{M(x)} + \frac{1}{2} \sum_{x \in \mathbb{X}} Q(x) \log \frac{Q(x)}{M(x)}$$

where  $P$  and  $Q$  are two probability distributions over  $\mathbb{X}$ ,  $M = 1/2 (P+Q)$ . Details about the algorithm are shown in Algorithm 2 in appendix. As before, we select the top-10%  $n$ -grams ranked by the divergence values as the candidate  $n$ -grams to filter in the input.

## 4.2 Adversarial Filtering

To further encourage more balanced learning, we adapt the adversarial filtering proposed by (Sakaguchi et al., 2019) to smooth the entity label distribution to prevent the model from learning only from the head of the distribution (frequent entities) but also from the tail of the distribution (rarer entities). The core idea of adversarial filtering is to filter out “easy” training examples — training

instances where their removal doesn’t negatively impact the model — to encourage the model to learn from the “hard” examples, through an iterative process utilizing weak linear learners.

During each iteration, we train 100 linear classifiers (logistic regression) on a randomly sampled subset (30%) of training instances. When the training of each classifier converges, we use it to make predictions for the remaining 70% instances and record their predictions. At the end of each iteration, we compute the average prediction accuracy for each instance by calculating the ratio of correct predictions over all classifiers, and filter out instances that have a prediction accuracy  $\geq 0.75$  and repeat the process with the remaining instances for the next iteration. The algorithm terminates when less than 500 instances are filtered during one iteration or when it has reached 100 iterations. After filtering, any instances that are not filtered are used to *further* fine-tune the entity predictor (BERT). Note that we apply this fine-tuning on the best model (based on validation) from contrastive learning (Section 4.1), and following previous studies (Tian et al., 2020; Chen et al., 2020; Khosla et al., 2021) we freeze the BERT parameters and initialise (randomly) a new linear layer.

## 5 Experiments

To verify the effectiveness of our proposed debiasing approach, we conduct a comprehensive study comparing our model against a number of benchmark systems. Our experiments include cross-domain/dataset generalization test, adversarial samples (created by distorting words and sentences), and utterances featuring unseen  $n$ -grams.

### 5.1 Datasets and Metrics

We use MultiWOZ (Eric et al., 2019) as the main dialogue dataset for our experiments. Specifically, we use version 2.2 of the dataset (Zang et al., 2020) which fixes a number of annotation errors and disallows slots with a large number of values to improve data quality. We use two popular metrics, BLEU and Entity F1 for evaluation.

### 5.2 Baselines

We compare our model against the following state-of-the-art benchmark systems: 1) Mem2Seq (Madotto et al., 2018): employs a recurrent network-based decoder to generate system responses and utilize memory networks to store

Model	Original		WP		WD		SP		SI	
	F1	BLEU	F1	BLEU	F1	BLEU	F1	BLEU	F1	BLEU
Mem2Seq (Madotto et al., 2018)	23.42	4.53	7.69	3.94	8.20	3.91	9.65	4.17	10.25	4.06
GLMP (Wu et al., 2019b)	33.79	6.22	10.21	5.34	10.97	5.29	13.14	5.69	14.04	5.53
DF-Net (Qin et al., 2020)	35.73	7.01	11.02	6.08	11.73	6.03	14.01	6.45	14.96	6.28
SimpleTOD (Hosseini-Asl et al., 2020)	35.80	20.20	11.19	9.25	12.02	9.19	14.37	10.63	15.35	10.45
Ours (w/o CL, w/ MLM) <sup>◇</sup>	<b>36.74</b>	<b>21.05</b>	11.33	10.99	12.67	10.97	15.01	11.53	16.47	12.24
Ours (w/ CL, Frequent $n$ -grams) <sup>♣</sup>	32.20	20.61	27.85	17.87	26.66	17.23	26.44	16.33	19.90	16.04
Ours (w/ CL, Mutual Information) <sup>♣</sup>	31.86	20.04	28.84	18.38	26.98	17.36	27.14	16.60	23.60	16.89
Ours (w/ CL, Jensen-Shannon Divergence) <sup>♣</sup>	31.50	19.42	29.15	18.96	28.13	18.33	28.95	17.81	23.96	17.37
Ours (w/o CL, w/ AF) <sup>♡</sup>	31.35	20.37	27.22	17.80	26.51	17.57	26.04	17.14	21.30	16.49
Ours (w/ CL, w/ AF) <sup>♡</sup>	30.98	19.26	<b>29.89</b>	<b>19.01</b>	<b>29.28</b>	<b>18.93</b>	<b>29.20</b>	<b>18.06</b>	<b>28.69</b>	<b>17.59</b>

Table 1: Adversarial attack results. All the models are trained on the original (unperturbed) MultiWOZ data using all domains. “Original” denote the original MultiWOZ test set, while “WP”, “WD”, “SP” and “SI” denote adversarial test sets created through word paraphrasing, word deletion, sentence paraphrasing and sentence insetion respectively, using NlpAug (Ma, 2019). <sup>◇</sup>: Our vanilla model without contrastive learning or adversarial filtering; <sup>♣</sup>: our model with contrastive learning; <sup>♡</sup>: our model with adversarial filtering.

the KB and copy KB entities from memory via pointer mechanism. The decoder are jointly trained with memory networks end-to-end by maximizing the likelihood of the final system responses; 2) GLMP (Wu et al., 2019b): employs a global-to-local pointer mechanism over the standard memory networks architecture for improving KB retrieval accuracy during response generation. The global pointer is supervised by additional training signals extracted from the standard system responses; 3) DF-Net (Qin et al., 2020): utilizes a shared-private architecture to capture both domain-specific and domain-general knowledge to improve the model transferability; 4) SimpleTOD (Hosseini-Asl et al., 2020): a causal language model based on GPT-2 trained on several task-oriented dialogue sub-tasks including dialogue state tracking, action prediction and response generation. It exploits additional training signals such as dialogue states and system acts compared to other systems.

### 5.3 Implementation Details

For delexicalized response generation, we use pretrained gpt2.<sup>4</sup> We use the default hyperparameter configuration, except for learning rate and batch size where we optimise via grid search. The learning rate is selected from  $\{1e^{-3}, 1e^{-4}, 1e^{-5}, 2e^{-3}, 2e^{-4}, 2e^{-5}\}$  and batch size from  $\{2, 4, 8, 16, 32\}$  based on the best validation performance. For entity prediction, we use pretrained bert-base-uncased.<sup>5</sup> During contrastive

<sup>4</sup><https://huggingface.co/gpt2>.

<sup>5</sup><https://huggingface.co/bert-base-uncased>.

pre-training stage, the learning rate is selected from  $\{1e^{-3}, 1e^{-4}, 1e^{-5}, 1e^{-6}\}$  and batch size from  $\{2, 4, 8, 16, 32\}$  using grid search based on validation performance. We pre-train BERT with contrastive learning for 20 epochs. The model with the best validation performance (minimum loss) is used for fine-tuning for entity prediction. During fine-tuning stage, the learning rate is selected from  $\{1e^{-3}, 1e^{-4}, 1e^{-5}, 2e^{-3}, 2e^{-4}, 2e^{-5}\}$  and the batch size from  $\{2, 4, 8, 16, 32\}$ . We use Adam (Kingma and Ba, 2014) as the optimizer. In terms of  $n$ -gram order,  $n = 3$  (trigram).

We run all experiments five times using different random seeds and report the average. All the models are trained on a single GeForce RTX 2080 Ti GPU and the training of both components (response generator and entity predictor) takes approximately one day.

### 5.4 Adversarial Attack Results

Language variety is one of the key features of human languages (Ganhotra et al., 2020), i.e., we tend to express the same meaning using different words. In real-world situations, users may use very different expressions than those in the training data. To test model robustness under such situations, we perform several perturbations on user utterances in the original test set to construct adversarial test examples. We use the widely-used nlpaug library (Ma, 2019) to augment the “regular” user utterances to generate four adversarial test sets through: word paraphrasing (WP), word deletion (WD), sentence paraphrasing (SP), and sentence insertion

Model	F1	BLEU
Mem2Seq (Madotto et al., 2018)	10.38	4.27
GLMP (Wu et al., 2019b)	14.25	5.84
DF-Net (Qin et al., 2020)	15.17	6.61
SimpleTOD (Hosseini-Asl et al., 2020)	15.57	12.79
Ours (w/o CL, w/ MLM) <sup>◇</sup>	15.82	14.36
Ours (w/ CL, Frequent $n$ -grams) <sup>♣</sup>	20.33	17.17
Ours (w/ CL, Mutual Information) <sup>♣</sup>	21.25	17.86
Ours (w/ CL, Jensen-Shannon Divergence) <sup>♣</sup>	26.42	21.83
Ours (w/o CL, w/ AF) <sup>♡</sup>	20.26	15.53
Ours (w/ CL, w/ AF) <sup>♡</sup>	<b>29.80</b>	<b>22.05</b>

Table 2: Unseen utterances generalization test results. All the training and inference are done on the new train/test splits (see Section 5.5) created to reduce  $n$ -gram overlap between training and test data. “F1”: testing F1 using all the domains; “BLEU”: testing BLEU using all the domains.

(SI). All the hyper-parameters of the augmentation tool `nlpaug` are kept to their default. We train all systems (benchmark and ours) using the *original* MultiWOZ and test them on both the original test set and adversarial test sets. Results are shown in Table 1.

Our model has several variants: (1) vanilla without any debiasing, noting that it still has domain adaptive pre-training using the masked language model loss ( $\diamond$ ); (2) with contrastive loss for domain-adaptive pre-training ( $\clubsuit$ ); and (3) with adversarial filtering, applied with or without contrastive pre-training ( $\heartsuit$ ). The reason why our vanilla model has masked language model pre-training is that we need to understand that when we introduce contrastive pre-training, any performance gain is attributed to the contrastive learning objective rather than the domain adaptive pre-training.

Looking at the original test set (“Original”), among the benchmark systems SimpleTOD is the best model, and our vanilla model ( $\diamond$ ) performs similarly (marginally better F1 and BLEU). Introducing contrastive learning ( $\clubsuit$ ) and adversarial filtering ( $\heartsuit$ ) somewhat degrades the entity prediction performance (F1), although the quality of the generated response (BLEU) is less impacted. Moving on to the adversarial test sets, all benchmark systems and our vanilla model observe severe performance degradation: F1 drops by over 20 points and BLEU by 10 points for most systems, suggesting that these models are not robust against perturbed inputs. Our systems with contrastive learning and/or adversarial filtering, on the other hand, look promising: the drop is substantially less severe, 2-3 points in terms

Model	<i>Hotel, Attraction, Train</i> → <i>Restaurant</i>	
	F1	BLEU
Mem2Seq (Madotto et al., 2018)	9.70	4.88
GLMP (Wu et al., 2019b)	13.22	6.75
DF-Net (Qin et al., 2020)	14.09	7.57
SimpleTOD (Hosseini-Asl et al., 2020)	14.46	13.78
Ours (w/o CL, w/ MLM) <sup>◇</sup>	14.95	14.23
Ours (w/ CL, Frequent $n$ -grams) <sup>♣</sup>	19.09	15.27
Ours (w/ CL, Mutual Information) <sup>♣</sup>	22.24	15.33
Ours (w/ CL, Jensen-Shannon Divergence) <sup>♣</sup>	23.14	15.68
Ours (w/o CL, w/ AF) <sup>♡</sup>	21.30	16.35
Ours (w/ CL, w/ AF) <sup>♡</sup>	<b>25.13</b>	<b>17.93</b>

Table 3: Cross-domain generalization results. “ $X \rightarrow Y$ ”: X denote the training domain(s) and Y the test domain. More domains’ results can be found in Table 6.

of F1 and BLEU. Interestingly, we also see that SI appears to be the most challenging test set as its performance is lowest. Comparing the three different criteria for ranking  $n$ -grams (frequent  $n$ -gram, mutual information and Jensen-Shannon divergence), Jensen-Shannon divergence appears to have the upper hand, suggesting that label information and both the presence *and* absence of an  $n$ -gram is important for uncovering shortcuts in the data.

## 5.5 Unseen Utterances Generalization Results

To test our model’s generalization capability under unseen scenario, we construct a new MultiWOZ split that aims to reduce  $n$ -gram overlap between training and test data. We first collect all  $n$ -gram types in the full data (training + test) and remove low frequency ( $< 10$ )  $n$ -grams, and then create two sets of  $n$ -grams based on their frequencies: “train” which contains the most frequent (70%)  $n$ -gram types and “test” for the remaining (30%). These two sets will decide whether an instance will be assigned to the training or test partition. That is, we iterate each instance from the full data and put it to the training partition if it only contains “train”  $n$ -gram, or the test partition if it has only “test”  $n$ -gram.<sup>6</sup>

Empirically, in the original MultiWOZ split the  $n$ -gram overlap ratio is 82.75%; our new split reduces this to 51.2%. This means that during testing, a model using our split will be exposed to utterances with more unseen phrases, and if the model exploits the spurious cues ( $n$ -grams) in the input it

<sup>6</sup>For instances containing both “train”  $n$ -grams and “test”  $n$ -grams, we put them to the training partition or test partition according to the majority type. If the numbers of “train”  $n$ -grams and “test”  $n$ -grams are equal for an instance, we put it to the training partition.

Model	MultiWOZ→SMD		MultiWOZ→SGD	
	F1	BLEU	F1	BLEU
Mem2Seq (Madotto et al., 2018)	9.06	8.01	4.34	3.48
GLMP (Wu et al., 2019b)	12.25	11.45	5.18	4.66
DF-Net (Qin et al., 2020)	13.07	12.51	5.63	5.36
SimpleTOD (Hosseini-Asl et al., 2020)	13.41	13.87	5.75	7.51
Ours (w/o CL, w/ MLM) <sup>♣</sup>	13.57	14.45	6.06	8.94
Ours (w/ CL, Frequent $n$ -grams) <sup>♠</sup>	19.01	15.25	9.44	10.07
Ours (w/ CL, Mutual Information) <sup>♠</sup>	20.32	15.44	9.79	10.38
Ours (w/ CL, Jensen-Shannon Divergence) <sup>♠</sup>	21.80	15.70	11.23	10.68
Ours (w/o CL, w/ AF) <sup>♡</sup>	20.44	15.43	9.73	10.25
Ours (w/ CL, w/ AF) <sup>◇</sup>	23.79	18.25	11.41	10.99

Table 4: Cross-dataset generalization results. “A→B”: a model is trained using train partition of dataset A and evaluated on the test partition of dataset B in a zero-shot manner.

will likely to perform poorly under this new split, as these cues are more likely to be absent.

We train all models using the new training partition and test them on the new test partition and present the results in Table 2. Looking at the models without debiasing, we find a similar observation where SimpleTOD and our vanilla model (◇) are the best performing models over different domains. When we introduce contrastive learning (♠) and adversarial filtering (♡), we see an improvement over all domains, with the best variant that combines both (“w/ CL, w/ AF”) improving over the vanilla model by a large margin, about 14% in Entity F1 and 8% in BLEU. Contrastive learning and adversarial filtering seem to provide complementary signal based on this experiment, as combining them both produces substantially better performance.

## 5.6 Cross-domain Generalization Results

We now test cross-domain generalization, where a model is tested using a domain that is not in the training data. We use the “leave-one-out” strategy for this, where a model is trained using all except one domain and tested using that unseen domain.<sup>7</sup> We present the results in Table 3.

We see similar observations here. Without any

<sup>7</sup>We conduct the entity prediction for cross-domain/cross-dataset experiments in a zero-shot manner both for our approach and all the baselines. Specifically, we use the training data from the source domain to construct the vocabulary of entities, and any unseen entities in the target (test) domain are ignored for our approach and all baselines (since we don’t have any representation/embeddings for them). No embeddings can be generated for these entities under the zero-shot cross-domain/cross-dataset settings since the vocabulary doesn’t include these entities.

debiasing, SimpleTOD and our vanilla have the best performances. When we incorporate contrastive learning and adversarial filtering, we see a strong improvement in terms of model robustness. As before, the best variant is one that combines both, and when compared to the vanilla model it improves F1 by 10–18 and BLEU by 2–5 points depending on the test domain. For contrastive learning, Jensen-Shannon divergence is again the best criterion for selecting  $n$ -grams. Adversarial filtering by itself is also fairly effective, although not as effective as the best contrastive model.

## 5.7 Cross-dataset Results

We now test the hardest setting: cross-dataset generalization. If a model “overfits” a dataset and relies on spurious correlations to perform a task, it will likely to perform very poorly in a new dataset of the same task. In this experiment, we train systems on MultiWOZ, and test them on two other popular datasets for task-oriented dialogues: SMD (Eric et al., 2017) and SGD (Rastogi et al., 2020). For SGD, it doesn’t have a database like SMD and MultiWOZ. Following (Rastogi et al., 2020), we collect the returned entities from the API queries during each dialogue as the database records to mimic the data settings of SMD and MultiWOZ.

The results are shown in Table 4. Both contrastive learning and adversarial filtering are effective methods to improve model robustness. The best contrastive model (“w/ Jensen-Shannon divergence”) improves F1 by 5–8 and BLEU by 1–2 points when compared to the vanilla model. Adversarial filtering by itself is also effective, although



the improvement is marginally smaller compared to the best contrastive model. Once again, combining both produces the best performance.

All in all these generalization tests reveal strikingly similar observations. To summarize: (1) our vanilla model that decomposes task-oriented dialogue generation into delexicalized response generation and entity prediction performs competitively with benchmark systems; (2) for contrastive learning, Jensen-Shannon divergence is consistently the best performer for ranking  $n$ -grams, implying that it is important to consider both the absence and presence of  $n$ -grams when determining their correlations with the labels; and (3) contrastive learning and adversarial filtering complement each other, and the most robust model is produced by incorporating both methods.

## 6 Conclusion

In this work, we propose a contrastive learning framework to debias task-oriented dialogue models by encouraging models to ignore these frequent phrases to focus on semantic words in the input. We also adapt adversarial filtering to our task to further improve model robustness. We conduct a series of generalization experiments, testing our method and a number of state-of-the-art benchmarks. Experimental results show that contrastive learning and adversarial filtering complement each other, and combining both produces the most robust dialogue model.

## 7 Limitations

Although our proposed approach performs significantly better than state-of-the-art baselines under out-of-distribution settings, the major limitation of this work is that the performance of our proposed approach slightly degrades under in-distribution scenarios (i.e., the original test set) compared to those baselines (Table 1). We think this is mainly due to the fact that by discarding the frequent phrases in the input utterances, the model may lose certain useful information which might be important for the in-distribution performance. An interesting question is how can we accurately remove the appropriate tokens for constructing positive examples while least affecting the in-domain performance? We will leave this for our future exploration.

## References

- Yonatan Belinkov, Adam Poliak, Stuart M. Shieber, Benjamin Van Durme, and Alexander M. Rush. 2019. [Don't take the premise for granted: Mitigating artifacts in natural language inference](#).
- Antoine Bordes, Y-Lan Boureau, and Jason Weston. 2017. [Learning end-to-end goal-oriented dialog](#). In *ICLR*.
- Ruben Branco, António Branco, João António Rodrigues, and João Ricardo Silva. 2021. [Shortcuted commonsense: Data spuriousness in deep learning of commonsense reasoning](#). In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, pages 1504–1521, Online and Punta Cana, Dominican Republic. Association for Computational Linguistics.
- Paweł Budzianowski, Tsung-Hsien Wen, Bo-Hsiang Tseng, Iñigo Casanueva, Stefan Ultes, Osman Ramadan, and Milica Gasic. 2018. [Multiwoz-a large-scale multi-domain wizard-of-oz dataset for task-oriented dialogue modelling](#). In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, pages 5016–5026.
- Ting Chen, Simon Kornblith, Mohammad Norouzi, and Geoffrey Hinton. 2020. [A simple framework for contrastive learning of visual representations](#).
- Wenhu Chen, Jianshu Chen, Pengda Qin, Xifeng Yan, and William Yang Wang. 2019. [Semantically conditioned dialog response generation via hierarchical disentangled self-attention](#). In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 3696–3709.
- Yun-Nung Chen, Dilek Hakkani-Tür, Gökhan Tür, Jianfeng Gao, and Li Deng. 2016. [End-to-end memory networks with knowledge carryover for multi-turn spoken language understanding](#). In *Interspeech*, pages 3245–3249.
- Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2018. [Bert: Pre-training of deep bidirectional transformers for language understanding](#). *arXiv preprint arXiv:1810.04805*.
- 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.
- Mihail Eric, Rahul Goel, Shachi Paul, Abhishek Sethi, Sanchit Agarwal, Shuyag Gao, and Dilek Hakkani-Tür. 2019. [Multiwoz 2.1: Multi-domain dialogue state corrections and state tracking baselines](#). *arXiv preprint arXiv:1907.01669*.

- Mihail Eric, Lakshmi Krishnan, Francois Charette, and Christopher D. Manning. 2017. [Key-value retrieval networks for task-oriented dialogue](#). In [Proceedings of the 18th Annual SIGdial Meeting on Discourse and Dialogue](#), pages 37–49.
- Jatin Ganhotra, Robert Moore, Sachindra Joshi, and Kahini Wadhawan. 2020. [Effects of naturalistic variation in goal-oriented dialog](#).
- Tianyu Gao, Xingcheng Yao, and Danqi Chen. 2021. [Simcse: Simple contrastive learning of sentence embeddings](#).
- Mor Geva, Yoav Goldberg, and Jonathan Berant. 2019. [Are we modeling the task or the annotator? an investigation of annotator bias in natural language understanding datasets](#).
- Marjan Ghazvininejad, Chris Brockett, Ming-Wei Chang, Bill Dolan, Jianfeng Gao, Wen-tau Yih, and Michel Galley. 2018. [A knowledge-grounded neural conversation model](#). In [Thirty-Second AAAI Conference on Artificial Intelligence](#).
- Dan Hendrycks, Kevin Zhao, Steven Basart, Jacob Steinhardt, and Dawn Song. 2021. [Natural adversarial examples](#).
- Ehsan Hosseini-Asl, Bryan McCann, Chien-Sheng Wu, Semih Yavuz, and Richard Socher. 2020. [A simple language model for task-oriented dialogue](#). [arXiv preprint arXiv:2005.00796](#).
- Xiao Huang, Jingyuan Zhang, Dingcheng Li, and Ping Li. 2019. [Knowledge graph embedding based question answering](#). In [Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining](#), pages 105–113. ACM.
- Andrew Ilyas, Shibani Santurkar, Dimitris Tsipras, Logan Engstrom, Brandon Tran, and Aleksander Madry. 2019. [Adversarial examples are not bugs, they are features](#).
- Prannay Khosla, Piotr Teterwak, Chen Wang, Aaron Sarna, Yonglong Tian, Phillip Isola, Aaron Maschiot, Ce Liu, and Dilip Krishnan. 2021. [Supervised contrastive learning](#).
- Diederik P Kingma and Jimmy Ba. 2014. [Adam: A method for stochastic optimization](#). [arXiv preprint arXiv:1412.6980](#).
- Wenqiang Lei, Xisen Jin, Min-Yen Kan, Zhaochun Ren, Xiangnan He, and Dawei Yin. 2018. [Sequicity: Simplifying task-oriented dialogue systems with single sequence-to-sequence architectures](#). In [Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics](#).
- Edward Ma. 2019. [Nlp augmentation](#). <https://github.com/makcedward/nlpaug>.
- Andrea Madotto, Chien-Sheng Wu, and Pascale Fung. 2018. [Mem2Seq: Effectively incorporating knowledge bases into end-to-end task-oriented dialog systems](#). In [Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics \(Volume 1: Long Papers\)](#), pages 1468–1478.
- R. Thomas McCoy, Ellie Pavlick, and Tal Linzen. 2019. [Right for the wrong reasons: Diagnosing syntactic heuristics in natural language inference](#).
- Yulei Niu, Kaihua Tang, Hanwang Zhang, Zhiwu Lu, Xian-Sheng Hua, and Ji-Rong Wen. 2021. [Counterfactual vqa: A cause-effect look at language bias](#).
- Timothy Niven and Hung-Yu Kao. 2019. [Probing neural network comprehension of natural language arguments](#).
- Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. 2002. [Bleu: a method for automatic evaluation of machine translation](#). In [Proceedings of the 40th annual meeting on association for computational linguistics](#).
- Baolin Peng, Chunyuan Li, Jinchao Li, Shahin Shayan-deh, Lars Liden, and Jianfeng Gao. 2020. [Soloist: Building task bots at scale with transfer learning and machine teaching](#). [arXiv preprint arXiv:2005.05298](#).
- Baolin Peng, Xiujun Li, Jianfeng Gao, Jingjing Liu, and Kam-Fai Wong. 2018. [Deep dyna-q: Integrating planning for task-completion dialogue policy learning](#). In [Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics \(Volume 1: Long Papers\)](#), pages 2182–2192.
- Jiaxin Qi, Yulei Niu, Jianqiang Huang, and Hanwang Zhang. 2020. [Two causal principles for improving visual dialog](#).
- Libo Qin, Xiao Xu, Wanxiang Che, Yue Zhang, and Ting Liu. 2020. [Dynamic fusion network for multi-domain end-to-end task-oriented dialog](#). In [Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics](#), pages 6344–6354, Online. Association for Computational Linguistics.
- Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, Ilya Sutskever, et al. 2019. [Language models are unsupervised multitask learners](#). [OpenAI blog](#), 1(8):9.
- Abhinav Rastogi, Xiaoxue Zang, Srinivas Sunkara, Raghav Gupta, and Pranav Khaitan. 2020. [Towards scalable multi-domain conversational agents: The schema-guided dialogue dataset](#).
- Keisuke Sakaguchi, Ronan Le Bras, Chandra Bhagavatula, and Yejin Choi. 2019. [Winogrande: An adversarial winograd schema challenge at scale](#).
- Yonglong Tian, Dilip Krishnan, and Phillip Isola. 2020. [Contrastive multiview coding](#).

- Aaron van den Oord, Yazhe Li, and Oriol Vinyals. 2019. [Representation learning with contrastive predictive coding](#).
- Petar Veličković, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Lio, and Yoshua Bengio. 2017. Graph attention networks. [arXiv preprint arXiv:1710.10903](#).
- Thomas Wolf, Victor Sanh, Julien Chaumond, and Clement Delangue. 2019. Transfertransfo: A transfer learning approach for neural network based conversational agents. [arXiv preprint arXiv:1901.08149](#).
- Chien-Sheng Wu, Steven Hoi, Richard Socher, and Caiming Xiong. 2020. Tod-bert: pre-trained natural language understanding for task-oriented dialogue. [arXiv preprint arXiv:2004.06871](#).
- Chien-Sheng Wu, Andrea Madotto, Ehsan Hosseini-Asl, Caiming Xiong, Richard Socher, and Pascale Fung. 2019a. Transferable multi-domain state generator for task-oriented dialogue systems. [arXiv preprint arXiv:1905.08743](#).
- Chien-Sheng Wu, Richard Socher, and Caiming Xiong. 2019b. [Global-to-local memory pointer networks for task-oriented dialogue](#). In [ICLR](#).
- Qi Wu, Peng Wang, Chunhua Shen, Anthony Dick, and Anton Van Den Hengel. 2016. Ask me anything: Free-form visual question answering based on knowledge from external sources. In [Proceedings of the IEEE conference on computer vision and pattern recognition](#).
- Chen Xing, Yu Wu, Wei Wu, Yalou Huang, and Ming Zhou. 2018. Hierarchical recurrent attention network for response generation. In [Thirty-Second AAAI Conference on Artificial Intelligence](#).
- Xiaoxue Zang, Abhinav Rastogi, Srinivas Sunkara, Raghav Gupta, Jianguo Zhang, and Jindong Chen. 2020. [Multiwoz 2.2 : A dialogue dataset with additional annotation corrections and state tracking baselines](#).
- Yichi Zhang, Zhijian Ou, and Zhou Yu. 2020. Task-oriented dialog systems that consider multiple appropriate responses under the same context. In [Proceedings of the AAAI Conference on Artificial Intelligence](#), volume 34, pages 9604–9611.
- Yizhe Zhang, Siqi Sun, Michel Galley, Yen-Chun Chen, Chris Brockett, Xiang Gao, Jianfeng Gao, Jingjing Liu, and Bill Dolan. 2019. Dialogpt: Large-scale generative pre-training for conversational response generation. [arXiv preprint arXiv:1911.00536](#).
- Victor Zhong, Caiming Xiong, and Richard Socher. 2018. Global-locally self-attentive dialogue state tracker. [arXiv preprint arXiv:1805.09655](#).

## A Spurious Cues In Task-oriented Dialogue Dataset

To unveil potential linguistic artifacts in task-oriented dialogue datasets, we first conduct an investigation on MultiWOZ (Budzianowski et al., 2018), which is widely used among task-oriented dialogue studies. By comparing the performance of a model trained using full dialogue history (e.g., *I need to find a moderately priced hotel*) and partial history containing only frequent phrases (e.g., *I need to*), it tells us if shortcuts exist in the dataset and the model has picked them up to solve the task. Note that these frequent phrases tend to be function words that don’t bear much meaning (e.g., *I need to*), and as such a model that can perform the task well using only them means it has not truly solved the task by capturing the underlying semantics of user utterances.

We experiment with two popular types of dialogue models based on GPT (SimpleTOD (Hosseini-Asl et al., 2020)) and recurrent networks (GLMP (Wu et al., 2019b)). We evaluate using Entity F1 (Eric et al., 2017) and BLEU (Papineni et al., 2002) metrics which are the two main metrics for assessing the performance of dialogue models. F1 measures the accuracy of the system’s ability to extract the correct entities from the knowledge base, while BLEU measures how much word overlap between the system-generated response and the ground truth response; higher score means better performance in both metrics. The results are shown in Table 5. As we can see, both models perform similarly under the two training settings, implying that there are shortcuts in the data (i.e., frequent phrases that correlate strongly with entities and responses), and the model has learned to exploit these cues for the task. Manual analysis reveals that 87% of the frequent phrases do not contain much semantic information: most of them are made up of function words such as *I’m looking for*, *I would like*, *I don’t care*, and *That is all*. These results suggest that these models did not solve the task by having any real natural language understanding.

Next we look into class imbalance, another source of dataset biases (Branco et al., 2021). We analyze the distribution of KB entities in the system responses, i.e., we tally how often each entity appears in the responses in MultiWOZ. We find that the entity distribution is highly skewed, with the top-10 “head entities” (i.e., the most frequent entities) accounting for approximately 64% of total

Model	Input Signals	F1	BLEU
SimpleTOD (Hosseini-Asl et al., 2020)	Full Input	35.80	20.20
SimpleTOD (Hosseini-Asl et al., 2020)	Frequent phrases only	34.33	19.63
GLMP (Wu et al., 2019b)	Full Input	33.79	6.22
GLMP (Wu et al., 2019b)	Frequent phrases only	32.68	6.18

Table 5: Performance of two dialogue models under two training settings: using full input or partial input containing only frequent phrases. F1 and BLEU measure the accuracy of entity prediction and quality of generated response respectively.

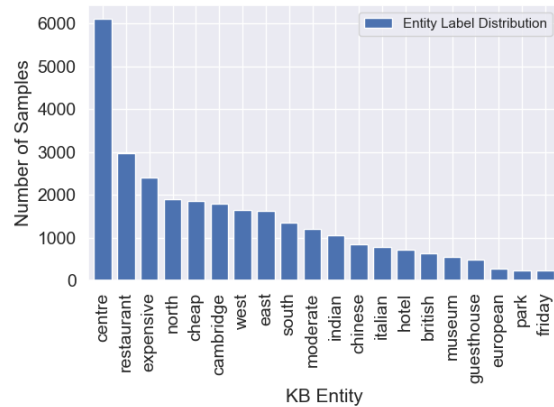


Figure 2: Entity label distribution on benchmark dataset MultiWOZ. X-axis denotes the top-20 most frequent entities in the system responses. Y-axis denotes the number of samples containing each entity.

occurrences, which means a large portion of the entities are in the (very) long tail of the distribution. The implication is that a model can simply focus on learning from a small number of head entities to achieve a high performance. Motivated by this observation, we adapt filtering algorithms to tackle this class imbalance issue, which works by smoothing the distribution so as to encourage our model to learn not only from the head of the distribution but also from the tail.

We focus on task-oriented dialogue data in this paper due to its data collection protocol. Since the data collection process of many task-oriented dialogue dataset is through a Wizard of Oz (WoZ) method and the topics between the two interlocutors are often constrained in few narrow domains (e.g., restaurant booking, hotel booking etc.), the languages used in these dialogues tend to be less diverse than open-domain dialogue corpus which often involves diverse topics in a single dialogue. Thus, task-oriented dialogue modelling might be more prone to be affected by the spurious correlations existed in the datasets. However, open-domain dialogue corpus and beyond are also worth



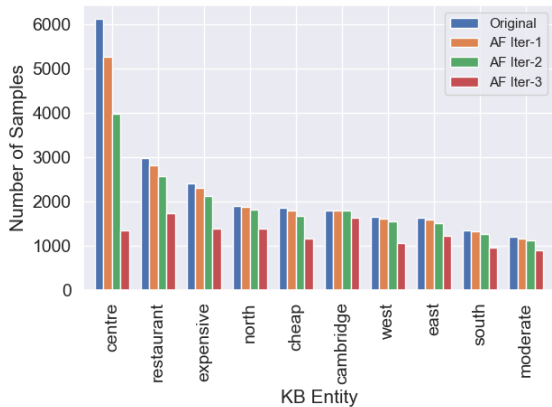


Figure 3: Change in entity frequency over different iterations of adversarial filtering. X-axis shows the 10 most frequent entity labels in the response. Y-axis shows the frequency of training instances for an entity. “Original”: Entity frequency without any filtering; “AF Iter-k”: Entity frequency after k iterations of filtering.

exploring whether the same or more types of spurious correlations exist in the dataset. We leave this for future exploration.

## B Adversarial Filtering Effects

The adversarial filtering iteratively detects the easy training instances and remove them. A natural question to ask is: why does this filtering process make the model more robust? To answer this question, we perform an analysis on the dynamics of the iterative process where we analyzed the number of instances containing a particular entity. We select the top-10 most frequent entities in the response and monitor their change in frequency over the iterations and present the results in Figure 3. As we can see from the figure, the distribution over these 10 entities has become “flatter” after the third iteration (red bars). The more frequent an entity is, the more instances are removed: at the extreme, the most frequent entity (*centre*) has lost almost 5000 instances after 3 iterations of filtering. Intuitively, we believe the more balanced distribution disincentivizes the model to focus on shortcuts that produce the frequent labels (entities), resulting in a model that learns generalisable patterns from a larger set of entities in the tail of the distribution.

Model	<i>Restaurant,Attraction,Train</i> → <i>Hotel</i>		<i>Restaurant,Hotel,Train</i> → <i>Attraction</i>		<i>Restaurant,Hotel,Attraction</i> → <i>Train</i>	
	F1	BLEU	F1	BLEU	F1	BLEU
Mem2Seq (Madotto et al., 2018)	2.87	3.89	6.97	3.67	2.89	3.03
GLMP (Wu et al., 2019b)	2.98	5.26	9.13	4.94	3.00	3.98
DF-Net (Qin et al., 2020)	3.32	5.99	9.79	5.66	3.34	4.65
SimpleTOD (Hosseini-Asl et al., 2020)	3.36	11.16	10.03	11.82	3.38	13.77
Ours (w/o CL, w/ MLM) <sup>◇</sup>	5.80	13.81	10.31	12.93	3.77	14.91
Ours (w/ CL, Frequent <i>n</i> -grams) <sup>▲</sup>	12.34	14.56	13.62	14.32	10.25	14.93
Ours (w/ CL, Mutual Information) <sup>▲</sup>	14.85	14.60	15.05	15.93	11.76	17.46
Ours (w/ CL, Jensen-Shannon Divergence) <sup>▲</sup>	18.01	15.01	19.61	16.38	12.48	18.86
Ours (w/o CL, w/ AF) <sup>▽</sup>	15.26	14.96	16.76	16.12	10.86	16.30
Ours (w/ CL, w/ AF) <sup>▽</sup>	<b>23.86</b>	<b>15.83</b>	<b>21.37</b>	<b>16.90</b>	<b>14.43</b>	<b>19.03</b>

Table 6: Cross-domain generalization results. “X→Y”: X denote the training domain(s) and Y the test domain. The result of Restaurant, Hotel, Attraction → Train is worse than other cross-domain generalization results. This may be due to that the entity set of “Train” domain is much larger than other domains (e.g., Restaurant, Hotel), thus making the entity prediction task more challenging than other domains. For examples, the slot “trainID” in “Train” domain contains 2462 values (e.g., “tr6161”, “tr8477”, “tr3498” etc.), which is much larger than slots in other domains (e.g., slot “area” in Restaurant domain only contains 5 values, i.e., south, west, centre, north, east).

---

**Algorithm 1:** Mutual information based bias identification

---

**Input** : dataset  $\mathcal{D} = (\mathbf{X}, \mathbf{y})$ ,  $n$ -gram size  $n$ , cutoff size  $k$

**Output** : biased tokens set  $\mathcal{S}$

- 1 Initialize  $n$ -grams distribution  $P_{ngrams} \leftarrow \emptyset$ ;
- 2 Initialize entity distribution  $P_{entity} \leftarrow \emptyset$ ;
- 3 Initialize ngrams-entity joint distribution  $P_{joint} \leftarrow \emptyset$ ;
- 4 Initialize mutual information values  $Q \leftarrow \emptyset$ ;
- 5 **foreach**  $(x, y) \in (\mathbf{X}, \mathbf{y})$  **do**
- 6      $ngrams \leftarrow \text{FindNgrams}(x, n)$ ;
- 7     **foreach** element  $e$  of the  $ngrams$  **do**
- 8         Add  $e$  to  $P_{ngrams}$ ;
- 9         Add  $y$  to  $P_{entity}$ ;
- 10        **forall**  $e \in ngrams$  **do** Add  $(e, y)$  to  $P_{joint}$ ;
- 11     **end**
- 12     **forall**  $(e_1, e_2) \in P_{joint}$  **do**
- 13         Calculate mutual information  $m$  of  $(e_1, e_2)$  using  $P_{ngrams}, P_{entity}, P_{joint}$  with Equation 4.1.2;
- 14         Add  $(e_1, e_2, m)$  to  $Q$ ;
- 15     **end**
- 16     Select the top- $k$  elements  $\mathcal{F}$  of  $Q$  and Add  $\mathcal{F}(e_1)$  to  $\mathcal{S}$ ;
- 17 **return**  $\mathcal{S}$

---

---

**Algorithm 2:** JSD based bias identification

---

**Input** : dataset  $\mathcal{D} = (\mathbf{X}, \mathbf{y})$ ,  $n$ -gram size  $n$ , cutoff size  $k$

**Output** : biased tokens set  $\mathcal{S}$

- 1 Initialize  $n$ -grams set  $S_{ngrams} \leftarrow \emptyset$ ;
- 2 Initialize positive entity distribution  $P_{positive} \leftarrow \emptyset$ ;
- 3 Initialize negative entity distribution  $P_{negative} \leftarrow \emptyset$ ;
- 4 Initialize JSD values  $Q \leftarrow \emptyset$ ;
- 5 **foreach**  $x \in \mathbf{X}$  **do**
- 6      $ngrams \leftarrow \text{FindNgrams}(x, n)$ ;
- 7     **foreach** element  $e$  of the  $ngrams$  **do**
- 8         Add  $e$  to  $S_{ngrams}$ ;
- 9     **end**
- 10     **foreach**  $(x, y) \in (\mathbf{X}, \mathbf{y})$  **do**
- 11         **foreach**  $e \in ngrams$  **do**
- 12             **if**  $e \in x$  **then** Add  $(e, y)$  to  $P_{positive}$ ;
- 13             **else** Add  $(e, y)$  to  $P_{negative}$ ;
- 14         **end**
- 15     **end**
- 16     **foreach**  $e \in S_{ngrams}$  **do**
- 17         Calculate JSD values  $v$  for  $e$  using  $P_{positive}, P_{negative}$  with Equation ??;
- 18         Add  $(e, v)$  to  $Q$ ;
- 19     **end**
- 20     Select the top- $k$  elements  $\mathcal{F}$  of  $Q$  and Add  $\mathcal{F}(e)$  to  $\mathcal{S}$ ;
- 21 **return**  $\mathcal{S}$

---