Learning Improvised Chatbots from Adversarial Modifications of Natural Language Feedback

Makesh Narsimhan Sreedhar
Mila
Université de Montreal
narsimma@mila.quebec

Kun Ni
Mila
Université de Montreal
nikun@mila.quebec

Siva Reddy
Facebook CIFAR AI Chair, Mila
McGill University
siva@cs.mcgill.ca

Abstract

The ubiquitous nature of chatbots and their interaction with users generate an enormous amount of data. Can we improve chatbots using this data? A self-feeding chatbot improves itself by asking natural language feedback when a user is dissatisfied with its response and uses this feedback as an additional training sample. However, user feedback in most cases contains extraneous sequences hindering their usefulness as a training sample. In this work, we propose a generative adversarial model that converts noisy feedback into a plausible natural response in a conversation. The generator’s goal is to convert the feedback into a response that answers the user’s previous utterance and to fool the discriminator which distinguishes feedback from natural responses. We show that augmenting original training data with these modified feedback responses improves the original chatbot performance from 69.94% to 75.96% in ranking correct responses on the PERSONA-CHAT dataset, a large improvement given that the original model is already trained on 131k samples.

1 Introduction

Enabling chatbots to indulge in engaging conversations requires massive datasets of human-human conversations (Ritter et al., 2011; Sordoni et al., 2015; Vinyals and Le, 2015; Zhang et al., 2018, 2019). Training such dialog agents requires substantial time and effort expended in the collection of adequate number of high quality conversation samples. Hancock et al. (2019) treat this feedback as a gold response to the wrong turn and use it as an additional training sample to improve the chatbot.

Although natural language feedback is cheap to collect from a chatbot’s end-users, most often, feedback cannot be used directly as a training sample since feedback is usually not the answer itself, but simply contains hints to the answer. Table 1 shows some feedback text samples. Naive modification of feedback using heuristics like regular expressions would lead to generic responses that are ineffective in improving the dialog ability of chatbots (Li et al., 2016). Additionally, writing an exhaustive set of regular expression rules is time consuming and requires extensive analysis of the data. Annotating data to convert feedback text to natural response is also expensive and defeats the purpose of learning from feedback text.

In this work, we propose a generative adversarial setup for converting such noisy feedback instances
you could say Hey, I'm 30, how old are you?
yes, I play battlefield would be a great answer
tell me what your favorite breakfast food is
answer the question about having children!

Table 1: Samples of feedback to the chatbot. These contain hints to the answer but they are not the answers themselves.

into natural, human-like responses that provide better training signals for the dialog agents. Figure 1 gives a bird’s-eye view of our problem. We frame this problem as a variant of text style transfer where the generator is tasked with making the feedback resemble a optimal response to the user’s previous utterance and the discriminator is a classifier that distinguishes whether a given response is feedback or not.

Our main contributions are the following:

- We introduce FEED2RESP, a text style transfer system that converts feedback to natural responses without full supervision, thus generating additional training samples (Section 2).

- We show that the training on FEED2RESP modified responses leads to improved accuracy of chatbots (Section 4). Our results also reveal that training naively on feedback doesn’t help when the original chatbot is already a strong model, whereas FEED2RESP also helps strong models.

2 Feedback to Natural Response Model

Hancock et al. (2019) introduce a novel variant of a self-feeding chatbot in which the dialogue agent is equipped with the capability of extracting new training samples while in conversation with humans after deployment (Figure 1). The agent also employs a satisfaction module which is trained to predict how satisfied the partner is with the responses it provides. When the chatbot is engaged in a conversation where the predicted satisfaction is below a defined threshold (usually 0.5), a feedback loop is triggered where the agent requests feedback from the human user on what should have been the response. The agent then utilizes the feedback text as the target response in new training examples for the primary dialogue ranking task. Hancock et al. (2019) show that this cost-efficient method of extracting new examples improves the chatbot’s dialogue abilities. In this work, we show that na"ıve use of the collected feedback is not necessarily a good technique and instead, we propose an approach to better utilize the collected feedback samples.

We pose the problem of converting feedback to resemble natural response as a text style transfer problem. We observe that feedback is more instructional and judgemental, whereas natural response is direct (answering questions) and engaging (asking questions, contains humor). We naturalize the feedback to a response and use it as an additional training sample to improve the chatbot.

A fully supervised approach to convert feedback to natural response is infeasible as we do not have paired (feedback ↔ response) examples and thus we adopt an adversarial setup. We utilize a GAN (Goodfellow et al., 2014) formulation where the generator modifies the feedback’s style to make it seem part of a natural conversation, and in turn fool the discriminator which knows how to distinguish natural responses and feedback. Our model, FEED2RESP, is shown in Figure 2.

2.1 Adversarial Setup

Given an input sentence $x$ (feedback or natural response) with source style $s$, conversation history $h$ and target style $\hat{s}$, the generator performs the mapping $g_{\theta} : (x, h, \hat{s}) \rightarrow \hat{y}$ (1)

Here $\hat{y}$ is the rewrite of $x$ into style $\hat{s}$. It is often the case that feedback and desired responses share many words (see Table 9). We use BART encoder-decoder initialized with pretrained weights as our generator since its denoising objective helps in copying from the input while also producing realistic sentences (Lewis et al., 2019). We additionally pretrain our model under the summarization setting to extract only the response when presented with conversation history and response. This helps maintain brevity while still integrating details from the context in the response.
The discriminator is a transformer encoder network that learns to distinguish the style of feedback and natural responses. Given an input text $x$ and conversation history $h$, it predicts the style class $c$ of $x$. Formally, it is defined as follows:

$$d_{\phi} : (x, h) \rightarrow c$$

(2)

### 2.2 Feed2Resp Learning

We train Feed2Resp on three main objectives: reconstruct sentences when the style is not changed, rewrite sentences from source to target style and ensure that the sentences retain their meaning when rewritten using different styles. These objectives are shown to work well in other style transfer scenarios (Dai et al., 2019).

**Self reconstruction objective** For the scenario where the target style is the same as the source style, we train the generator to reconstruct the sentence given as input. Considering the input sentence as $x$, the source and the target style as $s$, we minimize the negative log-likelihood loss to generate the same sentence $x$ as output.

$$Loss_{self}(\theta) = -\log p_{\theta}(\hat{y} = x|x, h, s)$$

(3)

**Cycle consistency objective** Taking inspiration from Cycle GAN (Zhu et al., 2017), we introduce a cycle consistency constraint to ensure that the model learns to preserve the meaning when it modifies the style of the original sentence. We first transform $x$ to style $\hat{s}$ to produce $\hat{y}$, i.e., $g_{\theta}(x, h, \hat{s})$. Subsequently, we feed as input $\hat{y}$ with the target style as $s$ and the model is trained to reconstruct the original sentence $x$. We minimize the negative log-likelihood loss which is given by:

$$Loss_{cycle}(\theta) = -\log p_{\theta}(y = x|g_{\theta}(x, h, \hat{s}), h, s)$$

(4)

**Style modification objective** To ensure that the style of an input sentence $x$ is changed to match the target one $\hat{s}$, we use the discriminator’s confidence as training signal. The generator wants to maximize the probability of the discriminator to classify transformed input to the target style, and therefore, we use the negative log-likelihood of the discriminator as our loss.

$$Loss_{style}(\theta) = -p_{\phi}(c = \hat{s}|g_{\theta}(x, h, \hat{s}))$$

(5)

### 2.3 End-to-end training

The discrete nature of sampling and non-differentiability of the argmax operator prevents gradient backpropogation. Following Dai et al. (2019), we consider the softmax distribution produced by the generator, $g_{\theta}$ as the ‘soft’ generated sentence and use it as input for further downstream networks to maintain differentiability.

### 3 Experimental Setup

In Feed2Resp, the optimizer for both the generator and discriminator is AdamW. The learning rate of generator is 5e-6 while the learning rate of discriminator is 1e-4. The discriminator uses 4 stacked transformer layers and 4 attention heads. The token embedding size, style embedding size, positional embedding size and hidden size are all 256. For the BART (Lewis et al., 2019) generator, we use the implementation from HuggingFace (Wolf et al., 2019) and initialize the model with pre-trained weights from the CNN/Daily Mail summarization task. Due to the characteristics of human response (refer Appendix A), we limit the length of text generation to a maximum of 50 words and impose a repetition penalty of 2.0 to improve diversity of output.

While evaluating the effectiveness of the modified feedback responses, we use two implementations of dialog agents provided by ParlAI (Miller et al., 2017), BiEncoder and PolyEncoder. BiEncoder has two transformer layers and 2 attention heads. The optimizer is Adamax with learning rate of 0.0025. PolyEncoder uses 12 transformer layers and 12 attentions heads. The optimizer is Adamax with learning rate of 5e-05.

The hyperparameters for the best performing model are arrived at by random sampling and subsequently verifying the outputs using human evaluation to rate the outputs from the style transfer task. The entire list of hyper-parameters is listed in the Table 8.

### 4 Experiments

Our goal is to test whether feedback helps improve the chatbot. To do this, we compare models trained on conversational data with and without feedback data. Below we describe the chatbot evaluation setting, our datasets, the main models and different settings of these models with and without feedback.

#### 4.1 Chatbot evaluation task and metrics

Following Hancock et al. (2019), we choose PersonaChat (Zhang et al., 2018) as the main evalua-
We train and test the above models in the following settings. Hancock et al. ignore the persona and just use the conversations to train chatbots and we follow the same approach. At test time, the model is presented the conversation history and 20 candidate responses and the model has to pick the correct response. Thus, we use HITS@1/20 metric for evaluation.

4.2 Feedback data

We use the feedback data collected by Hancock et al. (2019) as this removes orthogonal factors such as differences in chatbot interfaces and annotation framework etc. which are not the focus of this work. Hancock et al. collected this feedback by deploying bi-encoder chatbots (Section 4.3) trained on varying levels of training data and making it converse with crowdworkers. Whenever the bot’s response is not satisfactory, natural language feedback is collected from the crowdworker. The data thus collected contains 60k human-bot turns, of which the last turn is always the feedback.

4.3 Chatbot Models

Given the conversation history and several candidate responses, the chatbot is trained to rank the correct candidate on the top. We use the following models as our chatbots.

**BiEncoder** (Hancock et al., 2019; Humeau et al., 2020) contains two transformers, one for summarizing the conversation history and the other to summarize candidate responses to embeddings. The response with highest similarity is taken as the best candidate response.

**PolyEncoder** (Humeau et al., 2020) summarizes a context and candidate responses into several embeddings. In order to contextualize context and candidates together, it performs a cross-encoder attention on the summary embeddings and scores each candidate.

4.4 Feedback-based Models

We train and test the above models in the following settings.

**NOFeedback**: The model is trained only on human conversations.

**Feedback**: We train on the combination of human conversations and unmodified feedback data.

**Heuristic**: We design and use six regular expression rules based on the frequent patterns in the data that convert feedback to plausible dialog responses (see Appendix E) and train the chatbot models on human conversations along with the modified feedback.

**Feed2Resp**: We use our main model (Section 2) to modify feedback to natural responses and train the chatbot models on modified feedback along with human conversations.

### 5 Results and Discussion

The experimental details of the model variants are described in Section 3. Table 2 shows the average HITS@1/20 of all models on the PersonAChat validation and test sets over 3 runs. We were able to replicate results of Hancock et al. (2019) which show that BiEncoder performance improves slightly (+0.48 on test) when Feedback is used. Heuristic edits to feedback don’t help while Feed2Resp responses improve the results higher than Feedback and also have less variance. Coming to PolyEncoder, it is a much stronger chatbot than BiEncoder. We see that naive use of Feedback or Heuristic deteriorates the performance of PolyEncoder while Feed2Resp emerges a clear winner with +6.0 point improvement on the test set over NoFeedback.

**Feed2Resp analysis** We randomly sample 200 feedback responses from Feed2Resp to determine the kind of modifications the model performs (Table 3). We observe three main types of modifica-

<table>
<thead>
<tr>
<th>Model</th>
<th>Development</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>BiEncoder chatbot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOFeedback</td>
<td>49.03 (0.66)</td>
<td>49.49 (0.49)</td>
</tr>
<tr>
<td>Feedback</td>
<td>49.27 (1.06)</td>
<td>49.97 (1.30)</td>
</tr>
<tr>
<td>Heuristic</td>
<td>48.85 (0.70)</td>
<td>49.85 (0.72)</td>
</tr>
<tr>
<td>Feed2Resp</td>
<td>50.84 (0.50)</td>
<td>51.32 (0.43)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model</th>
<th>Development</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolyEncoder chatbot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOFeedback</td>
<td>73.35 (0.70)</td>
<td>69.94 (0.37)</td>
</tr>
<tr>
<td>Feedback</td>
<td>72.63 (0.14)</td>
<td>68.48 (0.64)</td>
</tr>
<tr>
<td>Heuristic</td>
<td>72.65 (0.35)</td>
<td>68.83 (0.31)</td>
</tr>
<tr>
<td>Feed2Resp</td>
<td>78.14 (0.40)</td>
<td>75.96 (0.80)</td>
</tr>
</tbody>
</table>
Figure 3: Attention maps for Feedback responses. Words such as you should have, you could have, tell me heavily influence the discriminator to classify it as feedback and hence the generator learns to remove such words to fool the discriminator. Darker shades of green mean higher attention scores and shades of red mean lower attention scores.

<table>
<thead>
<tr>
<th>Example</th>
<th>Freq.</th>
<th>Acc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>F: tell me about your favorite show</td>
<td>18.5%</td>
<td>81%</td>
</tr>
<tr>
<td>F2R: I love watching TV shows and sitcoms like friends</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification type: Remove</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F: you could’ve said, yes the sugar cinnamon kind is my favorite</td>
<td>40%</td>
<td>68.7%</td>
</tr>
<tr>
<td>F2R: yes the sugar cinnamon kind is my favorite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification type: Retain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F: the temperature is hot</td>
<td>41.5%</td>
<td>74.6%</td>
</tr>
<tr>
<td>F2R: the weather is hot</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Statistics of different modification types based on 200 random feedback texts. F stands for feedback, and F2R is the response of FEED2RESP model. Freq. indicates the frequency of the modification type, and Acc. the accuracy of FEED2RESP on each type. Appendix C lists additional examples of modified feedback responses.

6 Conclusion

In this work, we show that while chatbots can be improved using natural language feedback, converting feedback to natural responses that fit in the conversation outperform the naive usage of feedback. We presented FEED2RESP, a generative adversarial model, that converts feedback to natural responses without requiring manually annotated parallel data. Our results show that FEED2RESP results in a 6 point improvement for the POLYENCODE chatbot, an already powerful dialog ranking agent. This is a strong result as HITS@1/20 is a tough metric to improve upon (Hancock et al., 2019).

Our work joins the class of models that use natural language feedback to improve different tasks, e.g., image captioning (Ling and Fidler, 2017), classification (Srivastava et al., 2017; Hancock et al., 2018; Murty et al., 2020). While these methods use feedback for reward shaping or feature extraction, we use feedback to produce correct response using adversarial learning. We pose this problem as a style transfer problem inspired from the style transfer literature (Shen et al., 2017; Xu et al., 2018; Li et al., 2018; Conneau and Lample, 2019; Dai et al., 2019). While these focus on studying the stylistic attributes of sentences, e.g, sentiment, we explore this problem in the context of improving chatbots.

Acknowledgements

We thank Yue Dong for her helpful discussions during the course of this project. We also thank Sandeep Subramanian for his insightful guidance at a crucial stage of this work. This research was enabled in part by computations support provided by Compute Canada (www.computecanada.ca). The last author is supported by the NSERC Discovery Grant on Robust conversational models for accessing the world’s knowledge.
References


A Dataset Statistics

We are going to validate our approach on the chatbot’s performance using PERSONACHAT (Zhang et al., 2018) dialogue dataset and Human-Bot feedback dataset (Hancock et al., 2019). Table 6 reports the size of each dataset, all of which are available via ParlAI.²

<table>
<thead>
<tr>
<th>Task</th>
<th>Train</th>
<th>Valid</th>
<th>Test</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIALOGUE (HUMAN-HUMAN)</td>
<td>131438</td>
<td>7801</td>
<td>6634</td>
<td>145873</td>
</tr>
<tr>
<td>FEEDBACK (HUMAN-BOT)</td>
<td>60000</td>
<td>1000</td>
<td>1000</td>
<td>62000</td>
</tr>
</tbody>
</table>

Table 4: The number of examples used in our experiments by task and split. Note that the HH DIALOGUE examples come from the PERSONACHAT dataset, HB FEEDBACK examples from Hancock et al. (2019)

To train the FEED2RESP model, we take the entire FEEDBACK dataset and an equal number of randomly chosen samples from the DIALOGUE dataset. We them use a train-dev-test split of 0.8:0.1:0.1 for training and evaluation of the model.

<table>
<thead>
<tr>
<th>Task</th>
<th>Train</th>
<th>Valid</th>
<th>Test</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Style Transfer</td>
<td>96000</td>
<td>12000</td>
<td>12000</td>
<td>120000</td>
</tr>
</tbody>
</table>

Table 5: The number of samples per split used in our style transfer experiment. We take an equal number of samples from the FEEDBACK and DIALOGUE datasets and randomly shuffle them to create train, validation and test splits. The number of samples of each class in all the splits are ensured to be evenly distributed.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Human-Human Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Words in context (MEAN)</td>
<td>79 13</td>
</tr>
<tr>
<td>#Words in context (MEDIAN)</td>
<td>77 6</td>
</tr>
<tr>
<td>#Words per turn (MEDIAN)</td>
<td>10.7 7.1</td>
</tr>
<tr>
<td>#Words per turn (MEAN)</td>
<td>11 6</td>
</tr>
<tr>
<td>#Turns (MEAN)</td>
<td>4 1.5</td>
</tr>
</tbody>
</table>

Table 6: The number of words per context and per turn. The second part is the average number of turns in a conversation.

We examine the average number of turns and words in dialogues from the the feedback and human-human conversation distributions. We see that on an average, the dialogues in the feedback distribution have fewer number of turns than in human-human conversations. The average number of words per turn is also fewer on average.

B Preparation of Training Data

We use the dataset provided by Hancock et al. (2019), which is a cleaner version of PERSONACHAT dataset and comes with a new crowdsourced test set. We sample an equal number of examples from the DIALOGUE dataset, giving them a label 0, and FEEDBACK dataset, giving them a label of 1. The final response are combined with last n turns with an delimiter [RES]. Typically, n=2 turns are used for each conversation example. Conversation turns are separated with delimiter tokens [P1] or [P2].

C FEED2RESP examples

Here we include several examples of predictions from different models in Table 9.

D Computing Infrastructure and Runtime of Experiments

All experiments are conducted on Nvidia V100 GPUs. Average runtime of experiments is listed in Table 7 and assume running experiments on a single Nvidia V100 GPU.

<table>
<thead>
<tr>
<th>Task</th>
<th>Approximate Training Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>BiENCODER</td>
<td>16H</td>
</tr>
<tr>
<td>POLYENCODER</td>
<td>16H</td>
</tr>
<tr>
<td>FEED2RESP</td>
<td>48H</td>
</tr>
</tbody>
</table>

Table 7: Average runtime(in hours) of various experiments conducted

E Regular Expressions to modify FEEDBACK

As described in Section 4.4, we use the combination of following regular expressions to strip the filler words and extra choices in feedback data:

r"you could have|you should have|you could|you should"
r"ˆsaid|ˆsaying|ˆsay|ˆtell |ˆtold |ˆadmit |asked |ˆask |ˆanswer |ˆanswered |ˆtalked |ˆtalk "
r"ˆabout|ˆme|ˆthat"

r"if|whether|not|you are |to |i am |your |to |my |
you’ve |to |i’ve |
you were|to |i was |
you |to |i |

²https://parl.ai/projects/self_feeding/
<table>
<thead>
<tr>
<th>Model</th>
<th>layers</th>
<th>heads</th>
<th>optimizer</th>
<th>learning rate</th>
<th>#parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>BART Large</td>
<td>12</td>
<td>16</td>
<td>AdamW</td>
<td>5e-6</td>
<td>406M</td>
</tr>
<tr>
<td>Discriminator</td>
<td>4</td>
<td>4</td>
<td>AdamW</td>
<td>1e-4</td>
<td>16M</td>
</tr>
<tr>
<td>BIENCODER</td>
<td>2</td>
<td>2</td>
<td>Adamax</td>
<td>2.5e-3</td>
<td>23M</td>
</tr>
<tr>
<td>POLYENCODER</td>
<td>12</td>
<td>12</td>
<td>Adamax</td>
<td>5e-05</td>
<td>256M</td>
</tr>
</tbody>
</table>

Table 8: The hyperparameters used to obtain the results in Table 2.

Table 9: Examples of transformed feedback by our model, Feed2Resp, resulting in specific responses.