A Framework for Interactive Knowledge-Aided Machine Teaching

Karan Taneja∗, Harshvardhan Sikka and Ashok Goel
Georgia Institute of Technology
{karan.taneja, harshvardhan.sikka, ashok.goel}@cc.gatech.edu

Abstract

Machine Teaching (MT) is an interactive process where humans train a machine learning model by playing the role of a teacher. The process of designing an MT system involves decisions that can impact both efficiency of human teachers and performance of machine learners. Previous research has proposed and evaluated specific MT systems but there is limited discussion on a general framework for designing them. We propose a framework for designing MT systems and also detail a system for the text classification problem as a specific instance. Our framework focuses on three components i.e. teaching interface, machine learner, and knowledge base; and their relations describe how each component can benefit the others. Our preliminary experiments show how MT systems can reduce both human teaching time and machine learner error rate.

1 Introduction

Machine Teaching (MT) is an emerging discipline that focuses on understanding and building interfaces for human teachers engaged in teaching machine learners. An MT system allows human teachers to teach machine learners using an interactive interface to build a machine learning (ML) model. MT systems enable a wider community, beyond ML experts, to teach concepts to machine learners. According to Simard et al., 2017, MT systems should have intuitive, efficient, and friendly interfaces that decouple MT and ML processes such that the teaching does not require any knowledge of the underlying ML algorithms. Another advantage of MT is the cost reduction in creating ML models while improving their performance. Zhu et al., 2018, Liu et al., 2017, Zhu, 2015 studied MT as an optimization problem where learner performance needs to be maximized with minimum number of teaching examples. The optimization problem is given below where \( D \) is the dataset used for teaching, \( \theta \) represents ML model parameters and \( \eta \) is a scaling parameter.

\[
\min_{D, \theta} \text{TeachingRisk}(\theta) + \eta \cdot \text{TeachingCost}(D) \tag{1}
\]

In general, teaching risk measures the learner error, such as empirical risk on a test set, while teaching cost measures the resources, such as number of examples, used in teaching. Since MT systems involve many components acting together and influencing the learning outcomes, there is a need to develop a framework that lays out design principles for ideating MT systems. Our proposed MT framework consists of three main components: (i) teaching interface which describes the machine state exposed to teacher and the human feedback that will be asked from the teacher, (ii) machine learner which describes the feedback interpretation and ML algorithm(s), and (iii) knowledge base which describes the domain knowledge and task-specific knowledge used by the system. Our framework also proposes how these components will service each other and contribute towards the goals of machine teaching.

As we shall describe in detail later, we aim to minimize teaching risk by (i) allowing granular feedback and combining it with knowledge, (ii) using an adaptive machine learner which caters to online learning requirements and maximizes final performance, and (iii) prioritizing confusing examples using active learning. We also aim to minimize teaching cost by (i) exposing the machine state to human teacher using ideas from interpretable ML, (ii) using a knowledge base to assist human teaching, and (iii) suggesting valuable examples for human feedback.

In this paper, we also describe implementation of an MT system for text classification. We particularly address the task of intent classification for Jill Watson (JW) deployed in real-world classroom settings [Goel and Polepeddi, 2019]. An input to JW is classified into different intents for downstream processing in order to generate a response. For example, the question “How do I turn in assignment 1?” will be classified as ‘submission’, the question “How much time will it take to solve the exam 2?” will be classified as ‘estimated time’. An important use case of our work are such systems where multiple ML models may need to be trained and deployed as part of a bigger application. Each individual system can have an MT interface where a subject-matter expert can teach the machine to improve its performance using accumulated unlabeled examples over time.

The main contributions of this paper are: (i) we formalize a framework for designing MT systems by laying out its
components and their relations (Section 2), (ii) propose an MT system for text classification problem as a concrete instance of our framework (Section 3), and (iii) we quantify the improvements obtained in our initial experiments in terms of performance and time efficiency (Section 4).

2 Framework for MT System Design

In this section, we describe the main components of the proposed framework for designing MT systems (see Figure 1). The teaching interface allows the teacher to interact with the machine learner to train ML algorithms. This teaching process is supported by the knowledge base. Our aim is to keep the ML-expertise barrier low for human teachers while reducing the teaching cost and teaching risk. We also discuss previous work in the context of our framework in Section 5.

2.1 Teaching Interface

There are two main parts of a teaching interface: Machine State and Human Feedback.

Machine State: Machine state describes the information that is revealed to human teacher by the machine which helps the teacher in perceiving the machine learner’s state. Interpretable ML methods [Eiband et al., 2018; Das et al., 2020] can be used to form a better understanding of the machine learner for human teachers. This allows teachers to adapt their teaching practices as the machine learner improves.

Human Feedback: This describes the feedback that the teacher will provide to the machine. [Cui et al., 2021] defined four broad types of feedback i.e. showing, categorizing, sorting and evaluating. MT systems can employ one or more strategies to receive additional feedback on global as well as sub-input levels of granularity, such as token-level for input sentences or patch-level for images.

The teaching interface aids (i) the machine learner by providing data labels, granular feedback, etc., and (ii) the knowledge base by building task-specific information as well as missing domain knowledge.

2.2 Machine Learner

A machine learner is described by (i) the feedback interpretation mechanism used by the learner for exploiting feedback and (ii) the ML algorithms and related hyper-parameters.

Feedback Interpretation: A machine learner can accept feedback on different levels of granularity. Based on the feedback involved in teaching process, at least three feedback interpretation strategies that can be used are:

Input Features: If features can be engineered using human feedback, the machine learner can use them as inputs to the ML model [Godbole et al., 2004; Settles, 2011; Jandot et al., 2016].

Data Augmentation: The feedback can be used for data augmentation which can increase both performance and robustness of ML models [Rebuffi et al., 2021].

Loss Function Augmentation: The human feedback can be used to modify or augment loss functions. For instance, [Stiennon et al., 2020] and [Kreutzer et al., 2018] used human preferences as rewards in RL setting for text summarization and machine translation respectively. [He et al., 2016] asked simple questions to non-experts for parsing and used their answers for penalizing parser outputs.

ML Algorithms: As the machine learner receives a new teaching example, it needs to learn from it and present the new machine state to the teacher which requires online learning. The machine learner can use a faster and smaller model for online tasks and a more powerful model for the end application. Also, as more data is collected by the machine learner, it may need to adapt the underlying algorithm and/or related hyper-parameters to maximize its performance. The machine learner can use techniques like neural architecture search [Elkken et al., 2019] for this adaptive behavior.

In addition to learning the task at hand, the machine learner can aid human teaching in at least two ways:

ML Interpretability: The machine learner can provide its ‘interpretation’ of an unlabeled example to expose Machine State discussed in Section 2.1 [Simard et al., 2017] reasoned that human teachers using MT systems should not need an understanding of the underlying ML algorithm(s). We comply with this suggestion and also propose using model-agnostic interpretable ML for improving interaction with non-ML expert teachers.

Example Selection: Example selection is the process of ranking unlabeled examples that are displayed to the hu-
man. The machine can provide multiple unlabeled examples for feedback and rank them in order of decreasing confusion or increasing potential usefulness, such as in active learning [Settles, 2009]. Human teacher can use any example among these and provide feedback to the machine.

2.3 Knowledge Base

The knowledge base consists of domain-relevant information such as predefined probability distributions, rule-based systems, and any other tools. Using pre-trained generative neural networks is one powerful way to define a probability distributions over the problem domain i.e. the input space. Existing rule-based systems and other tools succinctly capture human expertise as procedural rules, relations, etc. Our text classification MT system (described in Section 3) illustrates specific use cases of the knowledge base. In general, the knowledge base can help MT system in two ways:

AIDING Teaching Interface: The teaching interface utilizes knowledge base to assist humans in efficiently communicating their expertise to the machine. For example, a word dictionary can be used to provide alternate word forms or synonyms that human teacher can use. In image domain, image inpainting models [Bertalmio et al., 2000] may recommend missing portions of an image.

AIDING Machine Learner: Domain knowledge and task-specific knowledge provided by the knowledge base can be used in augmenting human feedback for feedback interpretation by the machine learner. For example, data augmentation strategy can be supported by generative models or rule-based systems in text [Kobayashi, 2018; Wei and Zou, 2020], images [Frid-Adar et al., 2018] and other domains.

3 Implementation of an MT System for Text Classification

In this section, we specify our implementation of an MT system which employs our proposed framework. The goal of this implementation is to create an interface for teaching a machine learner about intent classification. The learned intent classifier will classify incoming inputs to JW into one of 26 possible intents. A sample interaction with our MT system implementation is given in Figure 2. In this example, input to JW is “How do I turn in an assignment?” and the correct intent is ‘submission’ since the input is inquiring about the submission process of an assignment, which is evident from the phrase ‘turn in’ in the input.

Teaching Interface: We built a command-line interface which has following two components:

Human Feedback: The human teacher provides (i) a label for the novel unlabeled example, (ii) marks words that are important, (iii) marks words that are inconsequential in determining the intent and (iv) validates alternate word and phrase replacements for the important words. In Figure 2 teacher provides ‘submission’ intent for the input, selects three words as inconsequential and two as important. The replacements validated by the teacher for the word ‘turn’ include ‘turn over’, ‘give’, ‘submit’, and ‘put’.

Machine State: Human teachers can judge machine state by observing (see example in Figure 2):

1. Model prediction on given unlabeled examples: Before accepting an example for teaching, the teacher can see the top-k predictions and corresponding confidence values. We used k = 5 in our experiments.
2. Word importance values: Before marking important and inconsequential words, the teacher can see importance values of words. (More details below.)
3. Recommended replacements: We use the knowledge base (described later) to help the teacher in feeding alternate words and phrases for important words.

How to calculate word importance values?: Importance value of a word is determined by deleting it from the input and measuring the Kullback–Leibler divergence [Kullback and Leibler, 1951] of the new output class distribution with the original distribution. A higher divergence means that a word was more important for determining the class distribution. This is inspired from [Ribeiro et al., 2016] who measured token importance values by scoring them with many
classifiers trained on input sentences where words were randomly removed. Our online system uses the fast simplified procedure described above to calculate importance values.

**Machine Learner – Feedback Interpretation:** We use the feedback from human teachers to augment data with two word replacement strategies. Firstly, for words marked as important by teacher, we generate sentence variations by replacing them with all the replacements validated by human teacher. For the example in Figure 2, the word ‘turn’ is replaced with ‘turn over’, ‘give’, ‘submit’, and ‘put’ to generate sentence variations. Secondly, for words marked as inconsequential, we replace them with the top three replacements recommended by BERT masked language model (LM) [Devlin et al., 2019] residing in the knowledge base. This is done by hiding the word with a '[MASK]' token, feeding it as input to BERT masked LM and using the three output words with the highest confidence corresponding to '[MASK]' token.

**Machine Learner – Algorithms:** We use bag-of-words perceptron model for (i) ranking unlabeled examples, and (ii) calculating word importance values displayed by teaching interface. The bag-of-words model trains in about 6-9 seconds and provides an online update since average labeling time (about 10 seconds) is more than the model update time. We also run architecture search [Elksen et al., 2019] in background to find better hyper-parameters based on the error on an evaluation set. For the results reported in Section 4, we fine-tune a pre-trained HuggingFace Tranformers model [Wolf et al., 2020] with a classification head. In particular, we used DistilBERT model [Sanh et al., 2019] which is a light-weight language model (40% smaller than BERT).

How are teaching examples selected? For example selection, we first reject the classes that have less than 1% confidence and calculate Shannon entropy over remaining classes. The examples with the highest entropy are presented to human teacher and teacher is free to accept or skip the example for teaching. This simple technique requires minimal computation and time, even for large unlabeled sample pools.

**Knowledge Base:** In our implementation, the knowledge base has three components:

BERT MASKED LM: A word can be replaced with '[MASK]' token and fed to BERT masked LM [Devlin et al., 2019] to get recommended replacements for assisting human teacher. In Figure 2 BERT provides some of the recommended replacements for word ‘turn’, such as ‘participate’ and ‘qualify’. The same model is also used for feedback interpretation as discussed earlier.

**WordNet and Word Forms:** To recommend synonyms for validation by human teacher in teaching interface, we used synonyms from WordNet and Python word_forms package. Some replacements for ‘turn’ in Figure 2 are recommended using this method, such as ‘turn over’ and ‘give’.

**Teacher Validated Replacements:** Word replacements validated by the teacher for important words are stored for future recommendations. In Figure 2 validated replacements ‘turn over’, ‘give’, ‘submit’, and ‘put’ will be recommended first when the word ‘turn’ is being replaced next time.

4 Experiments and Results

In this section, we describe our preliminary experiments and results. Our goal is to compare our MT implementation to regular labeling and active learning approaches.

**Dataset:** Our intent classification dataset has 28.1k examples which are generated by using 766 question templates labeled with intents. Each template contains placeholders for named entities. To generate examples, template placeholders are filled with a list of named entities relevant to problem domain. We used 162 templates to generate 5.6k examples which are used to bootstrap the machine learner. Remaining 22.5k examples are used as novel examples. Some examples and more details can be found in supplementary materials. Though this dataset is synthetic, it resembles use scenarios where users may be using similar inputs with different named entities. For measuring the performance of our system, we use a test set with 317 manually labeled examples acquired from deployments of JW [Goel et al., 2022].

**Experimenter Bias:** For experiments with our MT system, human feedback was collected from the first two authors as independent teachers, denoted by T1 and T2, in a total of 315 and 174 minutes respectively. This may have introduced a favorable bias in results because they knew the final metrics to be collected and the technical details of the system.

4.1 Comparison with Baselines

We compare two baselines with our MT system:

**Regular Labeling:** Traditionally, large amounts of data is collected and annotated before developing ML models. We simulate this data annotation process by including novel examples into the training dataset in random order and...
measuring error rate as number of seen examples increase.

**Active Learning:** In active learning, an ML algorithm scores the unlabeled data and constructs a query that includes most confusing examples. A human annotator labels the examples in the query and the ML algorithm is trained by including these newly labeled examples. We use the same active learning approach we used for example selection in our text classification MT system and simulate this data collection mechanism by including novel examples in the order of decreasing confusion into the training dataset.

Figure 3 shows the running-average classification error rate of two baseline methods and our MT system with T1 and T2 users with increase in (a) the number of examples and (b) time. In Figure 3, we observe that active learning performs better than regular labeling (11.2% relative decrease in error rate) as the number of examples are increased. Our MT system leads to fastest reduction in error rate with only 205 teaching examples for T1 and 216 examples for T2. We observe a 4.2% relative decrease in error rate compared to active learning and 14.9% compared to regular labeling. We estimated human time spent in labeling examples by asking T1 and T2 to label 75 randomly selected examples. We found that additional feedback costs about 8 × more time for T1 and 4 × for T2. Comparing human time cost (Figure 3), we observe that our MT system achieves the largest reduction in error rate. In the initial part of labeling process, regular labeling shows lowest running-average error rate because it samples a more diverse set of examples from the novel examples while active learning mechanism tends to give high confusion to similar examples. It is interesting that T2 spent almost half the time per example compared to T1 but achieved similar error rate improvements per unit time they spent (Figure 3b). Rest of the paper only uses data collected from T1 for brevity.

Each example taught using our MT system had a much higher impact on the classification performance than other two methods. We found that human feedback was used to create an average of 16 variations per example for T1. These are high-quality variations created by feedback interpretation mechanism using additional domain knowledge from BERT masked LM. We confirmed the quality of these variations by comparing with same amount of data generated using Easy Data Augmentation (EDA) technique [Wei and Zou, 2020] which involves random word insertions, swaps, deletions and synonym replacements. Using 16 variations per example generated using EDA, we observed a relative 11% increase in error rate (3.15% absolute error rate). We also note that we have not factored cognitive load in the teaching cost. Compared to our MT system, other baselines involve far more context switching since the teacher reviews 4-8× new examples in time they teach an example to the MT system.

### 4.2 Ablation Studies

Additional human feedback involves three parts: (i) highlighting inconsequential words that are not important in determining intent, (ii) highlighting important words that are important in determining intent and (iii) validating replacements for important words. We observed that T1 spent 19%, 9% and 72% of their time on above three tasks respectively. It took more time to highlight inconsequential words because human teachers likely think about inconsequential and important words jointly, but highlight the inconsequential words first. A very little time (about 1 second) was spent by T1 in skipping examples that were not deemed useful based on the example and intent predictions. On average, 1.16 examples were skipped for each accepted example.

In this subsection, we study each of these teaching sub-tasks and determine their importance using ablation experiments. We perform the following experiments:

- **Active Learning With Human Cooperation (AL+HC):** We use examples filtered by human teacher but do not use any additional feedback.
- **MT Without Important Words (MT-IW):** We use human feedback about inconsequential words and generate sentence variations by replacing them with words recommended by BERT masked LM.
- **MT Without Validated Word Replacements (MT-VWR):** We use feedback about both types of words. The inconsequential words are replaced as in MT-IW. The important words are replaced with intersection of BERT masked LM recommended words and WordNet synonyms.
- **Full MT (FullMT):** We use no ablations.

The results for above four experiments are presented in Figure 4. In terms of number of examples (Figure 4a), we observe that using validated word replacements (FullMT) leads to highest reduction in the error rate. Using feedback about inconsequential words (MT-IW) leads to a small improvement in performance over AL+HC. We find it interesting that MT-VWR leads to a small increase in the error rate over MT-IW. This suggests that dictionary synonyms are not necessar-
ily good replacements for important words and human validated replacements are valuable for lowering error rate.

In terms of human time (Figure 4), FullMT is comparable to the ablated systems. We believe that this is because FullMT allows efficient injection of knowledge into machine learner. It may also mean that spending more time on ablated versions may result in higher error rates (lower performance) because they lack injection of knowledge through validated replacements. To confirm this, we compared the best performing model generated by our MT system with same model trained on full dataset which has 28.1k examples, two orders of magnitude higher than number of teaching examples. The machine learner in our MT system outperforms the ML model trained using full data with a 0.94% reduction in the absolute error rate. This is a small improvement, but it suggests that human teaching can inject knowledge that is not captured by the unseen data into the machine learner.

5 Related Literature

Machine Teaching: [Simard et al., 2014] propose an interactive MT system for classification and information extraction. They also use active learning to allow teachers to interactively select teaching examples from a pool of sorted unlabeled examples. In addition to labels, human feedback also includes feature engineering. In follow-up work, [Ramos et al., 2020] focus on creating interactive and intuitive interface for non-ML expert teachers to teach machine learners. For information extraction tasks, teachers can create a hierarchy of extracted entities which is an additional source of feedback. To expose the machine state, they show errors in predictions on labeled examples in training set. Our work proposes a general approach for designing MT systems. We aim for better understanding of (i) human feedback for machine, through feedback interpretation, and (ii) machine learner for human, through interpretable ML. We also focus on knowledge base as a crucial component in assisting human teacher and augmenting teaching feedback.

[Zhu et al., 2018] study MT as an optimization problem where teaching risk and teaching cost are minimized as discussed earlier. [Liu et al., 2017] theoretically study scenarios where teacher provides an example by synthesizing or selecting it from a pool to reduce risk at each step. Our framework allows creative ways in which the interactive process of teaching can be made more efficient for both teacher and learner. We also allow selection of difficult examples through active learning and promote usefulness of examples by allowing granular human feedback to machine learner.

Human-in-the-loop (HITL) ML: [Cui et al., 2021] surveyed HITL ML and how design choices affect interactive learning. In their framework, they define four types of interaction: Showing, Categorizing, Sorting and Evaluating. Our current implementation uses Categorizing at two levels: sentence-level for labelling and word-level for marking important and inconsequential words. It also uses Showing in specifying alternate replacements for important words. In general, our framework allows elaborate feedback and more opportunities for feedback interpretation mechanisms.

HITL Text Classification: Previous work has explored HITL text classification for interactive annotation and feature engineering. [Godbole et al., 2004] created a user interface for text classification with active learning. Their interface allows human annotator to interactively engineer features for classifier and to see aggregate model statistics. [Settles, 2011] created a similar interface, additionally with an option to interactively label words with classes to use them as features. [Simard et al., 2014] [Jandot et al., 2016] focus on interactive interfaces for feature creation by human annotators in addition to labeling examples. [Wang et al., 2021] survey research in HITL natural language processing (NLP). Our framework is more general in terms of what feedback can be obtained from human teachers and how it can be used. In addition to this, we use knowledge base in our framework for augmenting feedback and for assisting teachers.

Data Augmentation: Data augmentation improves model performance by augmenting training examples with perturbed copies. In NLP, some common techniques include random word replacements, insertions, deletions, swaps, back-translating sentences to and from a second language [Sennrich et al., 2016], using LMs to generate sentence variations [Kolomiyets et al., 2011], [Kobayashi, 2018]. Our MT system implementation is an annotation tool relevant to early stages of ML development cycle and uses augmentation as a feedback interpretation mechanism. We use large pre-trained LMs as part of the domain knowledge and incorporate human feedback into it for generating variations of labeled examples in a limited data setting.

Active Learning: In active learning, an ML algorithm iteratively generates a query of examples for labelling by an oracle (such as human annotator) which leads to better performance with fewer training examples. For active learning with large unlabeled datasets in NLP, pool-based sampling methods [Settles, 2009] [Schröder and Niekler, 2020] are used where queries are constructed by sampling a pool of unlabeled examples. Common methods rely on model-based metrics like gradient magnitudes [Settles et al., 2007] or predictions-based metrics like entropy [Hwa, 2004], to select query from the sample pool. In our MT system, we use a naïve but fast entropy-based approach which helps in increasing learner’s performance and reduces human time spent.

6 Conclusion and Future Work

We proposed a framework for MT system design with teaching interface, machine learner and knowledge base as three main components. Each component benefits other components in many ways to reduce teaching risk and teaching cost. We presented a concrete example by implementing an MT system for text classification and discussed our results in a controlled experiment setting. Our next goal is to build an intuitive and friendly web-based interface and conduct experiments with unbiased subjects and datasets in public domain. We also wish develop and test MT systems for other domains, such as image and speech.

References

[Bertalmio et al., 2000] M Bertalmio, G Sapiro, V Caselles, et al. Image inpainting. In ACM SIGGRAPH, pages 417–
7 Supplementary Material

7.1 Training Dataset

Our training dataset for intent classification task is generated using templates for each intent. Some examples of intents and their templates are shown in Table 1. The name entities are inserted into placeholders marked by ‘{object}’. By iterating over a list of predefined entities for each placeholder, we generated a dataset for intent classification task.

We have a total of 26 intents with 766 templates which generated about 28.1k examples. About 20% of these templates were used to generate 5.6k examples for bootstrapping initial machine learner model and remaining 80% were used to generate data for machine teaching process.

| Intents            | Example Template                                      |
|--------------------|-------------------------------------------------------|
| submission         | How do I submit the {object}?                         |
| coursedescription  | Will we learn about {object} in this class?           |
| teachingstaff      | Who teaches this class?                               |
| officehours        | When are office hours this week?                      |
| lateworkpolicy     | What is the penalty for submitting work past the deadline? |
| importantdates     | When is the {object}?                                 |
| learning           | What are the learning goals of this class?            |
| courseprerequisites| Do we need to know {object} to take this course?       |
| definition         | Can you give an explanation for {object}?             |

Table 1: Examples of training templates used to generate training data.

7.2 Future Research Directions

Based on the machine state reported to the human teacher through the teaching interface, a teacher may choose different teaching strategies. An interesting future research direction would be to explore how different machine states affects human teaching and human performance. As an example, will revealing the error rate metric affect how teacher interacts with machine? Also, does the teacher spend less time on an example when its confusion score is low?

After understanding what different teaching behaviors imply, one can imagine building a mental model of human teacher in machine learner, leading to a mutual theory of mind. This mental model of teacher can be useful for machine learner in managing expectations and adapting its behavior.

It will also be interesting to find if spending more time per example in MT improves human performance and the quality of data. Additionally, one can ask if lower context switching, as compared to regular labeling where new examples are presented far more frequently, leads to lower cognitive load.