Automatic Essay Scoring Systems Are Both Overstable And Oversensitive: Explaining Why And Proposing Defenses

Yaman Kumar Singla*  
Adobe Media Data Science Research, IIT-Delhi, SUNY at Buffalo  
YKUMAR@ADOBE.COM

Swapnil Parekh*  
New York University  
SWAPNIL.PAREKH@NYU.EDU

Somesh Singh*  
IIT-Delhi  
F20180175@GOA.BITS-PILANI.AC.IN

Junyi Jessy Li  
University of Texas at Austin  
JESSY@AUSTIN.UTEXAS.EDU

Rajiv Ratn Shah  
IIT-Delhi  
RAJIVRATN@IIITD.AC.IN

Changyou Chen  
SUNY at Buffalo  
CHANGYOU@BUFFALO.EDU

Abstract

Deep-learning based Automatic Essay Scoring (AES) systems are being actively used by states and language testing agencies alike to evaluate millions of candidates for life-changing decisions ranging from college applications to visa approvals. However, little research has been put to understand and interpret the black-box nature of deep-learning based scoring algorithms. Previous studies indicate that scoring models can be easily fooled. In this paper, we explore the reason behind their surprising adversarial brittleness. We utilize recent advances in interpretability to find the extent to which features such as coherence, content, vocabulary, and relevance are important for automated scoring mechanisms. We use this to investigate the oversensitivity (i.e., large change in output score with a little change in input essay content) and overstability (i.e., little change in output scores with large changes in input essay content) of AES. Our results indicate that autoscoring models, despite getting trained as “end-to-end” models with rich contextual embeddings such as BERT, behave like bag-of-words models. A few words determine the essay score without the requirement of any context making the model largely overstable. This is in stark contrast to recent probing studies on pre-trained representation learning models, which show that rich linguistic features such as parts-of-speech and morphology are encoded by them. Further, we also find that the models have learnt dataset biases, making them oversensitive. The presence of a few words with high co-occurrence with a certain score class makes the model associate the essay sample with that score. This causes score changes in ~95% of samples with an addition of only a few words. To deal with these issues, we propose detection-based protection models that can detect oversensitivity and overstability causing samples with high accuracies. We find that our proposed models are able to detect unusual attribution patterns and flag adversarial samples successfully.

Keywords: Interpretability in AI, Automatic Essay Scoring, AI in Education

* Equal Contribution
1. Introduction

Automatic Essay Scoring (AES) systems are used in diverse settings such as to alleviate the workload of teachers, save time and costs associated with grading, and to decide admissions to universities and institutions. On average, a British teacher spends 5 hours in a calendar week scoring exams and assignments (Micklewright et al., 2014). This figure is even higher for developing and low-resource countries where the teacher to student ratio is dismal. While on the one hand, autograding systems effectively reduce this burden, allowing more working hours for teaching activities, on the other, there have been many complaints against these systems for not scoring the way they are supposed to (Feathers, 2019; Smith, 2018; Greene, 2018; Mid-Day, 2017; Perelman et al., 2014b). For instance, on the recently released automatic scoring system for the state of Utah, students scored lower by writing question-relevant keywords but higher by including unrelated content (Feathers, 2019; Smith, 2018). Similarly, it has been a common complaint that AES systems focus unjustifiably on obscure and difficult vocabulary (Perelman et al., 2014a). While earlier, each score generated by the AI systems was verified by an expert human rater, it is concerning to see that now they are scoring a majority of essays independently without any intervention by human experts (O’Donnell, 2020). The concerns are further alleviated by the fact that the scores awarded by these systems are used in life-changing decisions ranging from college and job applications to visa approvals (ETS, 2020b; Educational Testing Association, 2019; USBE, 2020; Institute, 2020).

Traditionally, autograding systems are built using manually crafted features used with machine learning based models (Kumar et al., 2019). Lately, these systems have been shifting to deep learning based models (Ke and Ng, 2019). For instance, many companies have started scoring candidates using deep learning based automatic scoring (SLTI-SOPI, 2021; Assessment, 2021; Duolingo, 2021; LaFlair and Settles, 2019; Yu et al., 2015; Chen et al., 2018; Singla et al., 2021; Riordan et al., 2017; Pearson, 2019). However, there are very few research studies on the reliability and validity of ML-based AES systems. More specifically, we have tried to address the problems of robustness and validity which plague deep learning based black-box AES models. Simply measuring test set performance may mean that the model is right for the wrong reasons. Hence, much research is required to understand the scoring algorithms used by AES models and to validate them on linguistic and testing criteria. Similar opinions are expressed by Madnani and Cahill (2018) in their position paper on automatic scoring systems.

With this in view, in this paper, we make the following contributions towards understanding current AES systems:

1) Several research studies have shown that essay scoring models are overstable (Yoon et al., 2018; Powers et al., 2002; Kumar et al., 2020; Feng et al., 2018). Even large changes in essay content do not lead to significant change in scores. For instance, Kumar et al. (2020) showed that even after changing 20% words of an essay, the scores do not change much. We extend this line of work by addressing why the models are overstable. Extending these studies further (§3.1), we investigate AES overstability from the perspective of context, coherence, facts, vocabulary, length, grammar and word choice. We do this by using integrated gradients (§2.2), where we find and visualize the most important words for scoring an essay (Sundararajan et al., 2017). We find that the models despite using rich contextual embeddings and deep learning architectures, are essentially behaving

---

1. A reliable measure is one that measures a construct consistently across time, individuals, and situations (Ramanarayanan et al., 2020).
2. A valid measure is one that measures what it is intended to measure (Ramanarayanan et al., 2020).
as bag-of-words models. Further, with our methods, we also able to improve the adversarial attack strength (§3.1.2). For example, for memory networks scoring model (Zhao et al., 2017), we delete 40% words from essays without significantly changing score (<1%), whereas Kumar et al. (2020) observed that deleting a similar number of words resulted in a decrease of 20% scores for the same model.

2) While there has been much work on AES overstability (Kumar et al., 2020; Perelman, 2014; Powers et al., 2001), there has been little work on AES oversensitivity. Building on this research gap, by using adversarial triggers, we find that the AES models are also oversensitive, i.e., small changes in an essay can lead to large change in scores (§3.2). We find that, by just adding 3 words in an essay containing 350 words (<1% change), we are able to change the predicted score by 50% (absolute). We explain the oversensitivity of AES systems using integrated gradients (Sundararajan et al., 2017), a principled tool to discover the importance of parts of an input. The results show that the trigger words added to an essay get unusually high attribution. Additionally, we find the trigger words have usually high co-occurrence with certain score labels, thus indicating that the models are relying on spurious correlations causing them to be oversensitive (§3.2.4). We validate both the oversensitive and overstable sample in a human study (§4). We ask the annotators whether the scores given by AES models are right by providing them with both original and modified essay responses and scores.

3) While much previous research in the linguistic field studies how essay scoring systems can be fooled, for the first time, we propose models that can detect samples causing overstability and oversensitivity (Pham et al., 2021; Kumar et al., 2020; Perelman, 2020). Our models are able to detect both overstability and oversensitivity causing samples with high accuracies (>90% in most cases) (§5). Also, for the first time in the literature, through these solutions, we propose a simple yet effective solution for universal adversarial perturbation (§5.1). These models, apart from defending AES systems against oversensitivity and overstability causing samples, can also inform effective human intervention strategy. For instance, AES deployments either completely rely on double scoring essay samples (human and machine) or solely on machine ratings alone (ETS, 2020a) can choose to have an effective middle ground. Using our models, AES deployments can select samples for human testing and intervention more effectively. Public school systems, e.g., in Ohio which use automatic scoring without any human interventions can select samples using these models for limited human intervention (O’Donnell, 2020; Institute, 2020). For this, we also conduct a small-scale pilot study on the AES deployment of a major language testing company proving the efficacy of the system (§5.3). Previous solutions for human interventions optimization rely on brittle features such as number of words and content modeling approaches like off-topic detection (Yoon et al., 2018; Yoon and Zechner, 2017). These models cannot detect adversarial samples like the ones we present in our work.

We perform our experiments for three model architectures and eight unique prompt 3 demonstrating the results on twenty four unique model-dataset pairs. It is worth noting that our goal in this paper is not to show that AES systems can be fooled easily. Rather, our goal is to interpret how deep-learning based scoring models score essays, why they are overstable and oversensitive, and how to solve the problems of oversensitivity and overstability.

---

3. Here a prompt denotes an instance of a unique question asked to test-takers for eliciting their opinions and answers in an exam. The prompts can come from varied domains including literature, science, logic and society. The responses to a prompt indicate the creative, literary, argumentative, narrative, and scientific aptitude of candidates and are judged on a pre-determined score scale.
dataset and tools for public use with the hope that it will spur testing and validation of AES models considering their huge impact on the lives of millions every year (Educational Testing Association 2019).

2. Background

2.1 Task, Models and Dataset

We use the widely cited ASAP-AES (2012) dataset which comes from Kaggle Automated Student Assessment Prize (ASAP) for the evaluation of automatic essay scoring systems. The ASAP-AES dataset has been used for automatically scoring essay responses by many research studies (Taghipour and Ng 2016; EASE 2013; Tay et al., 2018). It is one of the largest publicly available datasets (Table 1). The questions covered by the dataset span many different areas such as Sciences and English. The responses were written by high school students and were subsequently double-scored.

| Prompt Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---------------|---|---|---|---|---|---|---|---|
| #Responses    | 1783 | 1800 | 1726 | 1772 | 1805 | 1800 | 1569 | 723 |
| Score Range   | 2-12 | 1-6 | 0-3 | 0-3 | 0-4 | 0-4 | 0-30 | 0-60 |
| #Avg words per response | 350 | 350 | 150 | 150 | 150 | 150 | 250 | 650 |
| #Avg sentences per response | 23 | 20 | 6 | 4 | 7 | 8 | 12 | 35 |
| Type          | Argumentative | Argumentative | RC | RC | RC | RC | Narrative | Narrative |

Table 1: Overview of the ASAP AES Dataset used for evaluation of AS systems. (RC = Reading Comprehension).

We test the following two state-of-the-art models in this work: SkipFlow (Tay et al., 2018) and Memory Augmented Neural Network (MANN) (Zhao et al., 2017). Further, for comparison, we design a BERT based automatic scoring model. The performance is measured using Quadratic Weighted Kappa (QWK) metric, which indicates the agreement between a model’s and the expert human rater’s scores. All models show an improvement of 4-5% over the previous models on the QWK metric. The analysis of these models, especially BERT, is interesting in light of recent studies indicating that pre-trained language models learn rich linguistic features including morphology, parts-of-speech, word-length, noun-verb agreement, coherence, and language delivery (Conneau et al., 2018; Hewitt and Manning, 2019; Shah et al., 2021). This has resulted in pushing the envelope for many NLP applications. The individual models we use are briefly explained as follows:

**SkipFlow** (Tay et al., 2018) model essay scoring as a regression task. They utilize Glove embeddings for representing the tokens. SkipFlow captures coherence, flow and semantic relatedness over time, which the authors call neural coherence features. Due to the intelligent modelling, it gets an impressive average quadratic weighted kappa score of 0.764. SkipFlow is one of the top performing models (Tay et al., 2018; Ke and Ng, 2019) for AES.

**MANN** (Zhao et al., 2017) use memory networks for autoscoring by selecting some responses for each grade. These responses are stored in memory and then used for scoring ungraded responses. The memory component helps to characterize the various score levels similar to what a rubric does. They show an excellent agreement score of 0.78 average QWK outperforming the previous state-of-the-art models.
BERT-based We also design a BERT-based architecture for scoring essays. It utilizes BERT embeddings (Devlin et al., 2019) to represent essays by passing tokens through the BERT Encoder. The resultant embeddings from the last layer of the encoder are pooled and passed through a fully connected layer of size 1 to produce the score. The network was trained to predict the essay scores by minimizing the mean squared error loss. It achieves an average QWK score of 0.74. We also try out finetuning BERT to see its effect on downstream task (Mayfield and Black, 2020). It does not result in any statistically significant difference in results. We utilize this architecture as a baseline representative of transformer-based embedding models.

2.2 Attribution Mechanism

The task of attributing a score $F(x)$ given by an AES model $F$, on an input essay $x$ can be formally defined as producing attributions $a_1,..,a_n$ corresponding to the words $w_1,..,w_n$ contained in the essay $x$. The attributions produced are such that $\sum(a_1,..,a_n) = F(x)$, i.e., net attributions of all words ($\sum(a_1,..,a_n)$) equal the assigned score ($F(x)$). In a way, if $F$ is a regression based model, $a_1,..,a_n$ can be thought of as the scores of each word of that essay, which sum to produce the final score, $F(x)$.

We use a path-based attribution method, Integrated Gradients (IGs) (Sundararajan et al., 2017), much like other interpretability mechanisms such as (Ribeiro et al., 2016; Lundberg and Lee, 2017) for getting the attributions for each of the trained models, $F$. IGs employ the following method to find blame assignments: given an input $x$ and a baseline $b$, the integrated gradient along the $i^{th}$ dimension is defined as:

$$IG_i(x, b) = (x_i - b_i) \int_{\alpha=0}^{1} \frac{\partial F(b + \alpha(x - b))}{\partial x_i} d\alpha$$

where $\frac{\partial F(x)}{\partial x_i}$ represents the gradient of $F$ along the $i^{th}$ dimension of $x$.

We choose the baseline as empty input (all 0s) for essay scoring models since an empty essay should get a score of 0 as per the scoring rubrics. It is the neutral input that models the absence of a cause of any score, thus getting a zero score. Since we want to see the effect of only words on the score, any additional inputs (such as memory in MANN) of the baseline $b$ is set to be that of $x$. See Fig. 1 for an example.

We choose IGs over other explainability techniques since they have many desirable properties that make them useful for this task. For instance, the attributions sum to the score of an essay ($\sum(a_1,..,a_n) = F(x)$), they are implementation invariant, do not require any model to be retrained and are readily implementable. Previous literature such as (Mudrakarta et al., 2018) also uses Integrated Gradients for explaining the undersensitivity of factoid based question-answer (QA) models. Other interpretability mechanisms like attention require changes in the tested model and are not post-hoc, thus are not a good choice for our task.

4. Proposition 1 in (Sundararajan et al., 2017)
5. Defined as an input containing absence of cause for the output of a model; also called neutral input (Shrikumar et al., 2016; Sundararajan et al., 2017).
6. We ensure that IGs are within the acceptable error margin of <5%, where the error is calculated by the property that the attributions’ sum should be equal to the difference between the probabilities of the input and the baseline. IG parameters: Number of Repetitions = 20-50, Internal Batch Size = 20-50
Figure 1: Attributions for SkipFlow, MANN and BERT models respectively of an essay sample for Prompt 2. Prompt 2 asks candidates to write an essay to a newspaper reflecting their views on censorship in libraries and express their views if they believe that materials, such as books, etc., should be removed from the shelves if they are found offensive. This essay scored 3 out of 6.

3. Empirical Studies and Results

We perform our overstability (§3.1) and oversensitivity (§3.2) experiments with 100 samples per prompt for the three models discussed in Section 2.1. There are 8 prompt-level datasets in the overall ASAP-AES dataset, therefore we perform our analysis on 24 unique model-dataset pairs, each containing over 100 samples.

3.1 AES Overstability

We first present results on model overstability. Following the previous studies, we test the models’ overstability on different features important for AES scoring such as the knowledge of context (§3.1.1), coherence (§3.1.2), facts (§3.1.3), vocabulary (§3.1.4), length (§3.1.2), meaning (§3.1.3), and grammar (§3.1.4). This set of features provides an exhaustive coverage of all features important for scoring essays (Yan et al., 2020).

3.1.1 Attribution of Original Samples

We take the original human-written essays from the ASAP-AES dataset and do a word-level attribution of scores. Fig. 1 shows the attributions of all models for an essay sample from Prompt 2. We observe that SkipFlow does not attribute any word after the first few lines (first 30% essay content) of the essay while MANN attributions are spread over the complete length of the essay. For BERT-based model, we see that most of the attributions are over non-linguistic features (tokens) like ‘CLS’ and ‘SEP’. CLS and SEP tokens are used as delimiters in the BERT model. A similar result was also observed by Kovaleva et al. (2019).

For SkipFlow, we observe that if a word is negatively attributed at a certain position in an essay sample, it is then commonly negatively attributed in its other occurrences as well. For instance, books, magazines were negatively attributed in all its occurrences while materials, censored were positively attributed and library was not attributed at all. We could not find any patterns in the direction of attribution. In MANN, the same word changes its attribution sign when present in different essays. However, in a single instance of an essay, a word shows the same sign overall despite occurring in very different contexts.

Table 2 lists the top-positive, top-negative attributed words and the mostly unattributed words for all models. For MANN, we notice that the attributions are stronger for function words like, to,
of, you, do, and are and lesser for content words like, shelves, libraries, and music. SkipFlow’s top attributions are mostly construct-relevant words while BERT also focuses more on stop-words.

Figure 2: Variation of QWK with iterative addition of response words for SkipFlow, MANN and BERT models. The y-axis notes the relative QWK with respect to the original QWK and the x-axis represents iterative addition of attribute-sorted response words. These results are obtained on Prompt 7, similar results were obtained for all the prompts tested.

3.1.2 Iteratively Deleting Unimportant Words

For this test, we take the original samples and iteratively delete the least attributed words (Eq. 2).

\[
IG - \text{attribute sorted list of tokens} = (x_1, x_2, ..., x_k, ..., x_n)
\]

such that \(IG(x_1, b) > IG(x_2, b) > .. > IG(x_k, b)\), where \(x_k\) represents the \(k^{th}\) essay token to be removed, \(b\) represents the baseline and \(IG(x_k, b)\) represents the attribution on \(x_k\) with respect to baseline \(b\).

Through this, we note the model’s dependence on a few words without their context. Fig. 2 presents the results. We observe that the performance (measured by QWK) for the BERT model stays within 95% of the original performance even if one of every four words was removed from the essays in the reverse order of their attribution values. The percentage of words deleted were even more for the other models. While Fig. 1 showed that MANN paid attention to the full length of the response, removing words does not seem to affect the scores much. Notably, the words removed are not contiguous but interspersed across sentences, therefore deleting the unattributed words does not produce a grammatically correct response (see Fig. 3), yet can get a similar score thus defeating the whole purpose of testing and feedback.

These findings show that there is a point after which the score flattens out, i.e., it does not change in that region either by adding or removing words. This is odd since adding or removing a word from a sentence typically alters its meaning and grammaticality, yet the models do not seem to be affected; they decide their scores only based on 30-50% words. As an example, a sample after deleting bottom 40% attributed words is given here: “In the end patience rewards better than impatience. A time that I was patient was last year at cheer competition.”

3.1.3 Sentence and Word Shuffle

Coherence and organization are important features for scoring: they measure unity of different ideas in an essay and determine its cohesiveness in the narrative (Barzilay and Lapata, 2005). To check the dependence of AES models on coherence, we shuffle the order of sentences and words randomly and note the change in score between the original and modified essay (Fig. 3).
| Model | Positively Attributed Words |
|-------|-----------------------------|
| MANN  | to, of, are, ,, children, do,' we |
| SKIPFLOW | of, offensive, movies, censorship, is, our |
| BERT  | ,, the, to, and, ",, was, caps, [CLS] |

| Model | Negatively Attributed Words |
|-------|-----------------------------|
| MANN  | i, shelf, by, shelves, libraries, music, a |
| SKIPFLOW | the, i, to, in, that, do, a, or, be |
| BERT  | i, [SEP], said, a, in, time, one |

| Model | Mostly Unattributed Words |
|-------|-----------------------------|
| MANN  | t, you, the, think, offensive, from, my |
| SKIPFLOW | it, be, but, their, from, don't, one, what |
| BERT  | @, ##1, and, ,, my, patient |

Table 2: Top positive, negative and un-attributed words for SkipFlow, MANN and BERT-based model for Prompt 2.

We observe little change (<0.002%) in the attributions with sentence shuffle. The attributions are mostly dependent on word identities rather than their position and context for all models. We also find that shuffling sentences results in 10%, 2% and 3% difference in scores for SkipFlow, MANN, and BERT models, respectively. Even for these samples for which we observed a change in the scores, almost half of them increased their scores and the other half was reduced. The results are similar for word-level shuffling. This is surprising since change in the order of ideas in an essay alters the meaning of a prose but the models are unable to detect changes in either idea order or word-order. It indicates that despite getting trained as sentence and paragraph level models with the knowledge of language models, they have essentially become bag-of-words models.

Figure 3: Word-shuffled essay containing 40% of (top-attributed) words for SkipFlow (left), MANN (middle) and BERT (right) models respectively. The perturbed essay scores 26 (SkipFlow), 15 (MANN) and 5 (BERT) out of 30. The original essay was scored 25, 16, 4 respectively by the models.

3.1.4 Modification in Lexicon

Several previous research studies have highlighted the importance vocabulary plays in scoring and how AES models may be biased towards obscure and difficult vocabulary (Perelman et al., 2014a; Perelman 2014; Hesse, 2005; Powers et al., 2002; Kumar et al., 2020). To verify their claims, we replace the top and bottom 10% attributed words with ‘similar’ words.

7. Sampled from Glove with the distance calculated using Euclidean distance metric (Pennington et al., 2014)
Table 3 shows the results for this test. It can be noted that after replacing all the top and bottom 10% attributed words with their corresponding ‘similar’ words results in an average 4.2% difference in scores across all the models. These results imply that networks are surprisingly not perturbed by modifying even the most attributed words and produce equivalent results with other similarly-placed words. In addition, while replacing a word with a ‘similar’ word often changes the meaning and form of a sentence, the models do not recognize that change by showing no change in their scores.

| Result                                   | SkipFlow | MANN | BERT |
|------------------------------------------|----------|------|------|
| Avg score difference                     | 9.8%     | 2.4% | 3%   |
| % of top-20% attributed words which change attribution | 20.3%    | 9.5% | 34%  |
| % of bottom-20% attributed words which change attribution | 22.5%    | 26.0%| 45%  |

Table 3: Statistics obtained after replacing the top and bottom 10% attributed words of each essay with their synonyms.

Figure 4: Attributions for SkipFlow (left), MANN (middle) and BERT (right) models of an essay sample where a false fact has been introduced at the beginning. This essay sample scores (25/30, 18/30, 22/30) by the three models respectively. The original essay (without the added lie) scored (24/30), (18/30) and (21/30) respectively.

3.1.5 FACTUALITY, COMMON SENSE AND WORLD KNOWLEDGE

Factuality, common sense and world knowledge are important features in scoring essays (Yan et al., 2020). While a human expert can readily catch a lie, it is difficult for a machine to do so. We randomly sample 100 sample essays of each prompt from the ADDLIES test case of (Kumar et al., 2020). For constructing these samples, they used various online databases and appended the false information at various positions in the essay. These statements not only introduce false facts in the essay but also perturb its coherence.

A teacher who is responsible for teaching, scoring, and feedback of a student must have knowledge of world knowledge such as, ‘Sun rises in the East’, and ‘The world is not flat’. However, Fig. 4 shows that scoring models do not have the capability to check such common sense. The

---

8. For example, consider the replacement of the word ‘agility’ with its synonym ‘cleverness’ in the sentence ‘This exercise requires agility.’ does not produce a sentence with the same meaning.
models tested in fact attribute positive scores to statements like *the world is flat* if present at the beginning. These results are in contrast with studies like (Tenney et al., 2019; Zhou et al., 2020) which indicate that BERT and Glove like contextual representations have common sense and world knowledge. Ettinger (2020) in their ‘negation test’ also observe similar results to us.

**BABEL Semantic Garbage:** Linguistic literature has also reported that unexplicably, AES models give high scores to semantic garbage like the one generated using B.S. Essay Language Generator (BABEL generator)\(^9\) (Perelman et al., 2014a,b; Perelman, 2020). These samples are essentially semantic garbage with perfect spellings and obscure and lexically complex vocabulary. In stark contrast to (Perelman et al., 2014a) and the commonly held notion that writing obscure and difficult to use words fetch more marks, we observed that the models attributed infrequent words such as *forbearance*, *legerdemain*, and *propinquity* negatively while common words such as *establishment*, *celebration*, and *demonstration* were positively scored. Therefore, our results show no evidence for the hypothesis reported by studies like (Perelman, 2020) that writing lexically complex words make the AES systems give better scores.

### 3.2 AES Oversensitivity

While there has been literature for AES overstability, there is much less literature on AES oversensitivity. Therefore, next using universal adversarial triggers (Wallace et al., 2019), we show the oversensitivity of AES models. We add a few words (adversarial triggers) to the essays and cause them to have large changes in their scores. Post that, we attribute the oversensitivity to essay words and show that trigger words have high attributions and are the ones responsible for the model oversensitivity.

Through this, we test whether an automatically generated small phrase can perform an untargeted attack against a model to increase or decrease the predicted scores irrespective of the original input. Our results show that these models are vulnerable to such attacks, with as few as three tokens increasing / decreasing the scores of \(\approx 99\%\) of samples. Further, we show the performance of transfer attacks across prompts and find that \(\approx 80\%\) of them transfer, thus showing that the adversaries are easily domain adaptable and transfer well across prompt.\(^{10}\) We choose to use universal adversarial triggers for this task since they are input-agnostic, consist of a small number of tokens, and since they do not require the model’s white box access for every essay sample, they have the potential of being used as “cheat-codes” where a code once extracted can be used by every test-taker. Our results show that the triggers are highly effective.

#### 3.2.1 Adversarial Trigger Extraction

Following the procedure of Wallace et al. (2019), for a given trigger length (longer triggers are more effective, while shorter triggers are more stealthy), we initialize the trigger sequence by repeating the word “the” and then iteratively replace the tokens in the trigger to minimize the loss for the target prediction over batches of examples from any prompt \(p\).

This is a linear approximation of the task loss. We update the embedding for every trigger token \(e_{adv}\) to minimizes the loss’ first-order Taylor approximation around the current token embedding:

\[
arg_{e_i' \in \nu} \min_{e_i'} (e_i' - e_i)^T \nabla_{e_{adv}} L
\]  

\(^9\)https://babel-generator.herokuapp.com/
\(^{10}\) For the consideration of space, we only report a subset of these results.
Table 4: Single-prompt targeted attack performance results. Percentage of samples whose scores increase, Percentage of samples whose scores decrease on using triggers of length $c$ (Rows, Up to Down) on prompt $p$ (Columns, Left to Right) against Skipflow, BERT and MANN. The bold values denote the best values for each kind of attack on each prompt. (increasing, decreasing).

| Prompt→ | 1 | 4 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| Trigger Len | Model = SkipFlow | | | | |
| 3 | 68, 43 | 100, 14 | 86, 40 | 56, 81 | 43, 75 |
| 5 | 79, 38 | 100, 13 | 97, 42 | 65, 83 | 44, 78 |
| 10 | 85, 44 | 100, 18 | 100, 48 | 78, 88 | 55, 94 |
| 20 | 93, 68 | 100, 27 | 100, 58 | 90, 91 | 67, 99 |
| | Model = BERT | | | | |
| 3 | 71, 53 | 89, 31 | 66, 27 | 55, 77 | 46, 61 |
| 5 | 77, 52 | 90, 33 | 73, 33 | 58, 79 | 49, 64 |
| 10 | 79, 55 | 91, 41 | 87, 48 | 68, 84 | 55, 75 |
| 20 | 83, 61 | 94, 49 | 95, 59 | 88, 89 | 61, 89 |
| | Model = MANN | | | | |
| 3 | 67, 38 | 89, 15 | 86, 40 | 60, 80 | 41, 70 |
| 5 | 73, 39 | 93, 19 | 96, 42 | 61, 71 | 43, 77 |
| 10 | 85, 44 | 97, 20 | 99, 48 | 75, 84 | 59, 88 |
| 20 | 93, 63 | 100, 20 | 100, 59 | 84, 90 | 71, 94 |

Table 4: Single-prompt targeted attack performance results. Percentage of samples whose scores increase, Percentage of samples whose scores decrease on using triggers of length $c$ (Rows, Up to Down) on prompt $p$ (Columns, Left to Right) against Skipflow, BERT and MANN. The bold values denote the best values for each kind of attack on each prompt. (increasing, decreasing).

where $\nu$ is the set of all token embeddings in the model’s vocabulary and $\nabla_{\epsilon_{adv}} L$ is the average gradient of the task loss over a batch. We augment this token replacement strategy with beam search. We consider the top-k token candidates from Equation 3 for each token position in the trigger. We search left to right across the positions and score each beam using its loss on the current batch. We use small beam sizes due to computational constraints, increasing them may improve our results.

3.2.2 Experiments

We conduct two types of experiments namely Single prompt attack and Cross prompt attack.

**Single prompt attack** Given a prompt $p$, response $r$, model $f$, size criterion $c$, an adversary $A$ converts response $r$ to response $r'$ according to Eq. 3. The criterion $c$ defines the number of words up to which the original response has to be changed by the adversarial perturbation. We try out different values of $c$ ($\{3, 5, 10, 20\}$).

**Cross prompt attack** Here the adversarial triggers $A$ obtained from a model $f$ trained on prompt $p$ are tested against other model $f$ trained on prompt $p'$ (where $p' \neq p$).

3.2.3 Results

Here, we discuss the results of experiments conducted in the previous section.

**Single prompt attack** We found that the triggers can increase or decrease the scores very easily, with 3 or 5-word triggers being able to fool the model more than 95% of times correctly. It results in a mean increase of 50% on many occasions. Table 4 shows the percentage of samples that increase/decrease for various prompts and trigger lengths. The success of triggers increases with the
Figure 5: Single prompt attack for SkipFlow, BERT, Memory-Networks (§2.1). It shows the models’ predicted scores before and after adding 10-word triggers demonstrating the oversensitivity of these models subject to adversarial triggers. The green line indicates the scores given by a model not under attack, while the blue and red lines show the performance on attempting to increase and decrease the scores using the adversarial triggers.

Figure 6: Cross prompt attack for 20-word triggers obtained from SkipFlow trained on prompt 5 and tested on prompt 4 showing the transferability across prompts.

number of words as well. Fig. 5 shows a plot of predicted normalized scores before and after attack and how it impacts scores across the entire normalized score range. It shows that the triggers are successful for different prompts and models. As an example, adding the words “loyalty gratitude friendship” makes SkipFlow increase the scores of all the essays with a mean normalized increase of 0.5 (out of 1) (prompt 5) whereas adding “grandkids auditory auditory” decreases the scores 97% of the times with a mean normalized decrease of 0.3 (out of 1) (prompt 2).

Cross prompt attack We also found that the triggers are able to transfer easily, with 95% of samples increasing with a mean normalized increase of ~0.5 on being subjected to 3-word triggers obtained from attacking a different prompt. Fig. 5 shows a similar plot showing the success of triggers obtained from attacking prompt 5 and testing on prompt 4.

11. Other prompts had a similar performance so we have only shown a subset of results with one prompt of each type.
3.2.4 Trigger Analysis

We find that it is easier to fool the models to increase the scores than decrease it, with a difference of about 15% in their success (samples increased/decreased). We also observe that some of the triggers selected by our algorithm are very low frequency in the dataset and co-occur with only a few output classes (scores), thus having unusually high relative co-occurrence with certain output classes. We calculate pointwise mutual information (PMI) for such triggers and find that the most harmful triggers have the lowest PMI scores with the classes they effect the most (see Table 5).

| Prompt 4       | Score, Grade | PMI Value | Prompt 3      | Score, Grade | PMI Value |
|----------------|--------------|------------|---------------|--------------|------------|
| grass, 0       | 1.58         |            | write, 0      | 3.28         |            |
| conclusion, 0  | 1.33         |            | features, 0   | 3.10         |            |
| adopt, 3       | 1.86         |            | emotionally, 3| 1.33         |            |
| homesickness, 3| 1.78         |            | reservoir, 3  | 1.27         |            |
| wich, 1        | 0.75         |            | seeds, 1      | 0.93         |            |
| power, 2       | 1.03         |            | romshackle, 2 | 0.96         |            |

Table 5: PMI of trigger word-grade pairs for Prompt 4, 3. Other prompts also have similar results.

Further, we analyze the nature of triggers and find that a significant portion consists of archaic or rare words such as yawning, tallent, straggly with many foreign-derived words as well (wache, bibliothèque). We also find that decreasing triggers are 1.5x more repetitive than increasing triggers and contain half as many adjectives as the increasing ones.

4. Human Baseline

To test how humans perform on the different interpretability tests (§3.1, §3.2), we took 50 samples from each of overstability and oversensitivity tests and asked 2 human expert raters to compare the modified essay samples with the original ones. The expert raters have more than 5 years of experience in the field of language testing. We asked them two questions: (1) whether the score should change after modification and (2) should the score increase or decrease. These questions are easier to answer and produce more objective responses than asking the raters to score responses. We also asked them to give comments behind their ratings.

For all overstability tests except lexicon modification, both raters were in perfect agreement (kappa=1.0) on the answers for the two questions asked. They recommended (1) change in scores and that (2) scores should decrease. In most of the comments for the overstability attacks, the raters wrote that they could not understand the samples after modification. For oversensitivity causing samples, they recommended a score decrease but by a small margin due to little change in those samples. This clearly shows that the predictions of auto-scoring models are different from expert human raters and are yet unable to achieve human-level performance despite the recent claims that autoscoring models have surpassed human level agreement (Taghipour and Ng, 2016; Kumar and Boulanger, 2020; Ke and Ng, 2019).

12. All these words were already part of the model vocabulary.
13. For lexicon modification, the raters recommended the above in 78% instances with 0.85 kappa agreement.
5. Oversentivity and Overstability Detection

Next we propose detection-based solutions for oversensitivity (§5.1) and overstability (§5.2) causing samples. Here we propose detection based defence models to protect the automatic scoring models against potentially adversarial samples. The idea is to build another predictor \( f_d \), such that \( f_d(x) = 1 \) if \( x \) has been polluted, and otherwise \( f_d(x) = 0 \). Other techniques to tackle adversaries such as adversarial training have been shown to be ineffective against AES adversaries (Ding et al., 2020; Pham et al., 2021). It is noteworthy that we do not solve the general problem of cheating or dishonesty in exams, rather we solve the specific problem of oversensitivity and overstability adversarial attacks on AES models. Preventing cheating such as from copying from the web can be easily solved by proctoring or plagiarism checks. However, proctoring or plagiarism checks cannot solve the deep learning models’ adversarial behavior such as due to adding adversarial triggers or repetition and lexically complex tokens. It has been shown in both computer vision and natural language processing that deep-learning models inherently are adversarially brittle and protection mechanisms are required to make them secure (Zhang et al., 2020; Akhtar and Mian, 2018).

There is an additional advantage of detection-based adversaries. Most AES systems validate their scores with respect to humans post-deployment (ETS, 2020a; LaFlair and Settles, 2019). However, many deployed systems are now moving towards human-free scoring (ETS, 2020a; O’Donnell, 2020; LaFlair and Settles, 2019; SLTI-SOPI, 2021; Assessment, 2021). While it may have its advantages such as cost savings, but cheating in the form of overstability and oversensitivity causing samples are a major worry for both the testing companies and score users like universities and companies who rely on these testing scores (Mid-Day, 2017; Feathers, 2019; Greene, 2018). The detection based models provide an effective middle-ground where the humans only need to evaluate a few samples flagged by the detector models. A few studies studying this problem have been reported in the past (Malinin et al., 2017; Yoon and Xie, 2014). We also do a pilot study with a major testing company using the proposed detector models in order to judge their efficacy (§5.3). Studies on the same lines but with different motives have been conducted in the past (Powers et al., 2001, 2002).

5.1 IG Based Oversensitive Sample Detection

Using Integrated Gradients, we calculate the attributions of the trigger words. We found that, on average (over 150 essays across all prompts), attribution to trigger words is 3 times the attribution to the words in a normal essay (see Fig.7). This gave us the motivation to detect oversensitive samples automatically.

To detect the presence of triggers \( (y) \) programmatically, we utilize a simple 2 layer LSTM-FC architecture.

\[
\begin{align*}
    h_t, c_t &= L(h_{t-1}, c_{t-1}, x_t) \\
    y &= \text{Sigmoid}(w \ast h_t + b)
\end{align*}
\]

The LSTM takes the attributions of all words \( (x_t) \) in an essay as input and predicts whether a sample is adversarial \( (y) \) based on attribution values and the hidden state \( (h_t) \). We include an equal number of trigger and non-trigger examples in the test set. In the train set, we augment the data by including a single response with different types of triggers so as to make the model learn the attribution pattern of oversensitivity causing words. We train the LSTM based classifier such that there is no overlap between the train and test triggers. Therefore, the classifier has never seen the attributions of any samples with the test-set triggers. Using this setup, we obtained an average test
accuracy of 94.3% on a test set size of 600 examples per prompt. We do this testing over all the 24 unique prompt-model pairs. The results for 3 prompts (one each from argumentative, narrative, RC (see Table [1])) over the attributions of the BERT model are tabulated in Table [6]. As a baseline, we take a LSTM model which takes in BERT embeddings and tries to classify the oversensitivity causing adversarial samples using the embedding of the second-last model layer, followed by a dense classification layer. Similar results are obtained for all the model-prompt pairs.

| Model   | Prompt | Accuracy | F1  | Precision | Recall |
|---------|--------|----------|-----|-----------|--------|
| Baseline | 2      | 71       | 70  | 80        | 63     |
| IG-based| 2      | 90       | 91  | 84        | 99     |
| Baseline | 6      | 94       | 7490| 7491      | 784    | 7099   |
| IG-based| 6      | 99       | 94  | 93        | 90     | 96     |
| Baseline | 8      | 60       | 45  | 68        | 34     |
| IG-based| 8      | 99       | 99  | 98        | 96     | 100    |

Table 6: Validation metrics for IG attribution-based adversarial sample detection compared with Embedding-dense classification model for 3 representative prompts

Figure 7: Attributions for SkipFlow when adversarial triggers were inserted in the beginning. The figure shows high attributions on the trigger tokens irrespective of length of triggers.

5.2 Language Entropy Based Overstable Sample Detection

For overstability detection, we use a language model to find the text entropy. In psycholinguistics, it is well known that human language has certain fixed entropy (Frank and Jaeger, 2008). To maximize the usage of human communication channel, the number of bits per unit second remains constant (Frank and Jaeger, 2008; Jaeger, 2010). The principle of uniform information density is followed while reading, speaking, dialogues, grammar, etc (Jaeger, 2010; Frank and Jaeger, 2008; Jaeger, 2006). Therefore, semantic garbage (BABEL) or sentence shuffle and word modifications create unexpected language with high entropy. Thus, this inherent property of language can be used to detect overstable causing samples.

We use a GPT-2 language model (Radford et al., 2019) to do unsupervised language modelling on our training corpus to learn the grammar and structure of normal essays. We get the perplexity
score $P(x)$ of all essays after passing through GPT-2.

$$P(x) = e^{\tilde{H}(x)}$$ where \( \tilde{H}(x) = -\sum x q(x) \log_e p(x) \) (5)

where $p(x)$ and $q(x)$ are the estimated (by language model) and true probabilities of the word sequence $x$. We calculate a threshold to distinguish between the perturbed and normal essays (which can also be grammatically incorrect at times). For this, we use the Isolation Forest (Liu et al., 2008), which is a One class (OC) classification technique. Since OC classification only uses 1 type of examples to train, using only the normal essay perplexity, we can train it to detect when the perplexity is anomalous.

Scoring Function: $s(x, n) = 2^{-E(h(x))/c(n)}$ (6)

where $E(h(x))$ is the mean value of depths a single data point, $x$, reaches in all trees.

Normalizing Factor $c(n) = 2H(n - 1) - (2(n - 1)/n)$ (7)

where $H(i)$ = harmonic number = $\ln(i) + 0.5772$ (Euler’s constant) and $n$ is number of points used to construct trees.

We train this IsoForest model on our training perplexities and then test it on our validation set, i.e., other normal essays, shuffled essays (§3.1.3), lexicon-modified essays (§3.1.4) and BABEL samples (§3.1.5). The contamination factor of the IsoForest is set to 1%, corresponding to the number of probable anomalies in the training data. We obtain near perfect accuracies, indicating that our language model has indeed captured the language of a normal essay. Table 7 presents results on three representative prompts (one each from argumentative, narrative, RC (see Table 1)).

| Prompt | Normal Essays | Shuffle | Synonyms | BABEL |
|--------|---------------|---------|----------|--------|
| 2      | 99.1          | 100     | 82.5     | 100    |
| 6      | 99.6          | 98      | 80       | 100    |
| 8      | 99.3          | 98.9    | 83       | 100    |

Table 7: IsoForest accuracy on normal essays, shuffled essays (§3.1.3), lexicon-modified essays (§3.1.4) and BABEL samples (§3.1.5) for three representative prompts

5.3 Pilot Study

To test how well the sample detection systems work in practice, we conduct a small-scale pilot study using essay prompts of a major language testing company. We asked 3 experts and 20 candidate test-takers to try to fool the deployed AES models. The experts had an experience of more than 15 years in the field of language testing and were highly educated (masters in language and above). The test-takers were college graduates from the population served by the company. They were duly compensated for their time according to the local market rate. We provided them with our overstability and oversensitivity tests for their reference.

The pilot study revealed that the test-takers used several strategies to try to bypass the system like using semantic garbage such as what is generated from BABEL generator, sentence and word repetitions, bad grammar, second language use, randomly inserting trigger words, trigger word repetitions, using pseudo and non-words like jabberwocky, and partial question repeats. The models
Reason and Defenses against Overstability and Oversensitivity of AES Systems

reported were able to catch most of the attacks including the ones with repetitions, trigger words, pseudo and non-word usages, and semantic garbage with high accuracy (0.89 F1 with 0.92 recall scores on an average). However, bad-grammar and partial question repeats were difficult to recognize and identify (0.48 F1 score with 0.52 recall scores on an average). This is especially so since bad grammar could be indicative of both language proficiency and adversaries. While bad grammar was easily detected in semantic garbage category but it was detected with low accuracy when only a few sentences were off. Similarly, candidates often use partial question repeats to start or end answers. Therefore, it forms a construct-relevant strategy and hence cannot be rejected according to rubrics. This problem should be addressed in essay-scoring models by introducing appropriate inductive biases. We leave this task for future works.

6. Related Work

Automatic essay scoring: Almost all the auto-scoring models are learning-based and treat the task of scoring as a supervised learning task (Ke and Ng 2019) with a few using reinforcement learning (Wang et al. 2018) and semi-supervised learning (Chen et al. 2010). While the earlier models relied on ML algorithms and hand-crafted rules (Page 1966; Faulkner 2014; Kumar et al. 2017; Persing et al. 2010), lately the systems are shifting to deep learning algorithms (Taghipour and Ng 2016; Grover et al. 2020; Dong and Zhang 2016). Approaches have ranged from finding the hierarchical structure of documents (Dong and Zhang 2016), using attention over words (Dong et al. 2017), and modelling coherence (Tay et al. 2018). In this paper, we interpret and test the recent state-of-the-art scoring models which have shown the best performance on public datasets (Tay et al. 2018; Zhao et al. 2017).

AES testing and validation: Although automatic scoring has seen much work in recent years, model validation and testing still lag in the ML field with only a few contemporary works (Kumar et al. 2020; Pham et al. 2021; Yoon and Xie 2014; Malinin et al. 2017). Kumar et al. (2020) and Pham et al. (2021) show that AES systems are adversarially unsecure. Pham et al. (2021) also try adversarial training and obtain no significant improvements. Yoon and Xie (2014) and Malinin et al. (2017) model uncertainty in automatic scoring systems. Most of the scoring model validation work is in the language testing field, which unfortunately has limited AI-expertise (Litman et al. 2018). Due to this, studies have noted that the results there are often conflicting in nature (Powers et al. 2001, 2002; Bejar et al. 2013, 2014; Perelman 2020).

7. Conclusion and Future Work

Automatic scoring, one of the first tasks to be automated using AI (Whitlock 1964), is now shifting to black box neural-network based automated systems. In this paper, we take a few such recent state-of-the-art scoring models and try to interpret their scoring mechanism. We test the models on various features considered important for scoring such as coherence, factuality, content, relevance, sufficiency, logic, etc and explain the models’ predictions. We find that the models do not see an essay as a unitary piece of coherent text but as a bag-of-words. We find out why essay scoring models are both oversensitive and overstable and propose detection based protection models against such attacks. Through this, we also propose an effective defence against the recently introduced universal adversarial attacks.
Apart from contributing to the discussion of finding effective testing strategies, we hope that our exploratory study initiates further discussion about better modeling automatic scoring and testing systems especially in a sensitive area like essay grading.

References

Naveed Akhtar and Ajmal Mian. Threat of adversarial attacks on deep learning in computer vision: A survey. *IEEE Access*, 6, 2018.

ASAP-AES. The Hewlett foundation: Automated essay scoring develop an automated scoring algorithm for student-written essays. [https://www.kaggle.com/c/asap-aes/](https://www.kaggle.com/c/asap-aes/), 2012.

Truenorth Speaking Assessment. Truenorth speaking assessment: The first fully-automated speaking assessment with immediate score delivery. [https://emmersion.ai/products/truenorth/](https://emmersion.ai/products/truenorth/), 2021.

Regina Barzilay and Mirella Lapata. Modeling local coherence: An entity-based approach. In *Proceedings of the 43rd Annual Meeting of the Association for Computational Linguistics (ACL'05)*. Association for Computational Linguistics, 2005. doi: 10.3115/1219840.1219858.

Isaac I Bejar, Waverely VanWinkle, Nitin Madnani, William Lewis, and Michael Steier. Length of textual response as a construct-irrelevant response strategy: The case of shell language. *ETS Research Report Series*, 2013(1), 2013.

Isaac I Bejar, Michael Flor, Yoko Futagi, and Chaintanya Ramineni. On the vulnerability of automated scoring to construct-irrelevant response strategies (cirs): An illustration. *Assessing Writing*, 22, 2014.

Lei Chen, Jidong Tao, Shabnam Ghaffarzadegan, and Yao Qian. End-to-end neural network based automated speech scoring. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2018, Calgary, AB, Canada, April 15-20, 2018*. IEEE, 2018. doi: 10.1109/ICASSP.2018.8462562.

Yen-Yu Chen, Chien-Liang Liu, Chia-Hoang Lee, Tao-Hsing Chang, et al. An unsupervised automated essay-scoring system. *IEEE Intelligent systems*, 25(5), 2010.

Alexis Conneau, German Kruszewski, Guillaume Lample, Loïc Barrault, and Marco Baroni. What you can cram into a single $&!#*$ vector: Probing sentence embeddings for linguistic properties. In *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. Association for Computational Linguistics, 2018. doi: 10.18653/v1/P18-1198.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 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)*. Association for Computational Linguistics, 2019. doi: 10.18653/v1/N19-1423.
Yuning Ding, Brian Riordan, Andrea Horbach, Aoife Cahill, and Torsten Zesch. Don’t take “nswvtnvagxpm” for an answer – the surprising vulnerability of automatic content scoring systems to adversarial input. In *Proceedings of the 28th International Conference on Computational Linguistics*. International Committee on Computational Linguistics, 2020. doi: 10.18653/v1/2020.coling-main.76.

Fei Dong and Yue Zhang. Automatic features for essay scoring – an empirical study. In *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 2016. doi: 10.18653/v1/D16-1115.

Fei Dong, Yue Zhang, and Jie Yang. Attention-based recurrent convolutional neural network for automatic essay scoring. In *Proceedings of the 21st Conference on Computational Natural Language Learning (CoNLL 2017)*. Association for Computational Linguistics, 2017. doi: 10.18653/v1/K17-1017.

Duolingo. The duolingo english test: Ai-driven language assessment. [https://emmersion.ai/products/truenorth/](https://emmersion.ai/products/truenorth/) 2021.

Edx EASE. Ease (enhanced ai scoring engine) is a library that allows for machine learning based classification of textual content. this is useful for tasks such as scoring student essays. [https://github.com/edx/ease](https://github.com/edx/ease) 2013.

ETA Educational Testing Association. A snapshot of the individuals who took the gre revised general test, 2019.

ETS. Frequently asked questions about the toefl essentials test. [https://www.ets.org/s/toefl-essentials/score-users/faq/](https://www.ets.org/s/toefl-essentials/score-users/faq/) 2020a.

ETS. Gre general test interpretive data. [https://www.ets.org/s/gre/pdf/gre_guide_tablela.pdf](https://www.ets.org/s/gre/pdf/gre_guide_tablela.pdf) 2020b.

Allyson Ettinger. What BERT is not: Lessons from a new suite of psycholinguistic diagnostics for language models. *Transactions of the Association for Computational Linguistics*, 8, 2020. doi: 10.1162/tacl_a_00298.

Adam Faulkner. Automated classification of stance in student essays: An approach using stance target information and the wikipedia link-based measure. In *The Twenty-Seventh International Flairs Conference*, 2014.

Todd Feathers. Flawed algorithms are grading millions of students’ essays. [https://www.vice.com/en/article/pa7dj9/flawed-algorithms-are-grading-millions-of-students-essays](https://www.vice.com/en/article/pa7dj9/flawed-algorithms-are-grading-millions-of-students-essays) 2019.

Shi Feng, Eric Wallace, Alvin Grissom II, Mohit Iyyer, Pedro Rodriguez, and Jordan Boyd-Graber. Pathologies of neural models make interpretations difficult. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 2018. doi: 10.18653/v1/D18-1407.
Austin F Frank and T Florain Jaeger. Speaking rationally: Uniform information density as an optimal strategy for language production. In *Proceedings of the annual meeting of the cognitive science society*, volume 30, 2008.

Peter Greene. Automated essay scoring remains an empty dream. [https://www.forbes.com/sites/petergreene/2018/07/02/automated-essay-scoring-remains-an-empty-dream/?sh=da976a574b91](https://www.forbes.com/sites/petergreene/2018/07/02/automated-essay-scoring-remains-an-empty-dream/?sh=da976a574b91), 2018.

Manraj Singh Grover, Yaman Kumar, Sumit Sarin, Payman Vafaee, Mika Hama, and Rajiv Ratn Shah. Multi-modal automated speech scoring using attention fusion. *arXiv preprint arXiv:2005.08182*, 2020.

Douglas D Hesse. 2005 cccc chair’s address: Who owns writing? *College Composition and Communication*, 57(2), 2005.

John Hewitt and Christopher D. Manning. A structural probe for finding syntax in word representations. 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)*. Association for Computational Linguistics, 2019. doi: 10.18653/v1/N19-1419.

Thomas B. Fordham Institute. Ohio public school students. [https://www.ohiobythenumbers.com/](https://www.ohiobythenumbers.com/), 2020.

T Florian Jaeger. Redundancy and reduction: Speakers manage syntactic information density. *Cognitive psychology*, 61(1), 2010.

Tim Florian Jaeger. *Redundancy and syntactic reduction in spontaneous speech*. PhD thesis, Stanford University Stanford, CA, 2006.

Zixuan Ke and Vincent Ng. Automated essay scoring: A survey of the state of the art. In *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI 2019, Macao, China, August 10-16, 2019*. ijcai.org, 2019. doi: 10.24963/ijcai.2019/879.

Olga Kovaleva, Alexey Romanov, Anna Rogers, and Anna Rumshisky. Revealing the dark secrets of BERT. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*. Association for Computational Linguistics, 2019. doi: 10.18653/v1/D19-1445.

Vivekanandan Kumar and David Boulanger. Explainable automated essay scoring: Deep learning really has pedagogical value. In *Frontiers in Education*, volume 5. Frontiers, 2020.

Yaman Kumar, Swati Aggarwal, Debanjan Mahata, Rajiv Ratn Shah, Ponnurangam Kumaraguru, and Roger Zimmermann. Get IT scored using autosas - an automated system for scoring short answers. In *The Thirty-Third AAAI Conference on Artificial Intelligence, AAAI 2019, The Thirty-First Innovative Applications of Artificial Intelligence Conference, IAAI 2019, The Ninth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2019, Honolulu, Hawaii, USA, January 27 - February 1, 2019*. AAAI Press, 2019. doi: 10.1609/aaai.v33i01.33019662.
Yaman Kumar, Mehar Bhatia, Anubha Kabra, Jessy Junyi Li, Di Jin, and Rajiv Ratn Shah. Calling out bluff: Attacking the robustness of automatic scoring systems with simple adversarial testing. *arXiv preprint arXiv:2007.06796*, 2020.

Geoffrey T LaFlair and Burr Settles. Duolingo english test: Technical manual. *Retrieved April, 28, 2019.*

Diane Litman, Helmer Strik, and Gad S Lim. Speech technologies and the assessment of second language speaking: Approaches, challenges, and opportunities. *Language Assessment Quarterly, 15*(3):294–309, 2018.

Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 eighth ieee international conference on data mining*. IEEE, 2008.

Scott M. Lundberg and Su-In Lee. A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, 2017.

Nitin Madnani and Aoife Cahill. Automated scoring: Beyond natural language processing. In *Proceedings of the 27th International Conference on Computational Linguistics*. Association for Computational Linguistics, 2018.

Andrey Malinin, Anton Ragni, Kate Knill, and Mark Gales. Incorporating uncertainty into deep learning for spoken language assessment. In *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*. Association for Computational Linguistics, 2017. doi: 10.18653/v1/P17-2008.

Elijah Mayfield and Alan W Black. Should you fine-tune BERT for automated essay scoring? In *Proceedings of the Fifteenth Workshop on Innovative Use of NLP for Building Educational Applications*. Association for Computational Linguistics, 2020. doi: 10.18653/v1/2020.bea-1.15.

John Micklewright, John Jerrim, Anna Vignoles, Andrew Jenkins, Rebecca Allen, Sonia Ilie, Elodie Bellarbre, Fabian Barrera, and Christopher Hein. Teachers in england’s secondary schools: Evidence from talis 2013. 2014.

Mid-Day. What?! students write song lyrics and abuses in exam answer sheet. *https://www.mid-day.com/articles/national-news-west-bengal-students-write-song-lyrics-abuses-in-exam-answer-sheet/18210196*, 2017.

Pramod Kaushik Mudrakarta, Ankur Taly, Mukund Sundararajan, and Kedar Dhamdhere. Did the model understand the question? In *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. Association for Computational Linguistics, 2018. doi: 10.18653/v1/P18-1176.

Patrick O’Donnell. Computers are now grading essays on ohio’s state tests. *https://www.cleveland.com/metro/2018/03/computers_are_now_grading_essays_on_ohios_state_tests_your_ch.html*, 2020.

Ellis B Page. The imminence of... grading essays by computer. *The Phi Delta Kappan, 47*(5), 1966.
Jeffrey Pennington, Richard Socher, and Christopher Manning. GloVe: Global vectors for word representation. In Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP). Association for Computational Linguistics, 2014. doi: 10.3115/v1/D14-1162.

Les Perelman. When “the state of the art” is counting words. Assessing Writing, 21, 2014.

Les Perelman. The babel generator and e-rater: 21st century writing constructs and automated essay scoring (aes). The Journal of Writing Assessment, 13, 2020.

Les Perelman, Louis Sobel, Milo Beckman, and Damien Jiang. Basic automatic b.s. essay language generator (babel). https://babel-generator.herokuapp.com/ 2014a.

Les Perelman, Louis Sobel, Milo Beckman, and Damien Jiang. Basic automatic b.s. essay language generator (babel) by les perelman, ph.d. http://lesperelman.com/writing-assessment-robo-grading/babel-generator/ 2014b.

Isaac Persing, Alan Davis, and Vincent Ng. Modeling organization in student essays. In Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing. Association for Computational Linguistics, 2010.

Thang Pham, Trung Bui, Long Mai, and Anh Nguyen. Out of order: How important is the sequential order of words in a sentence in natural language understanding tasks? In Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021. Association for Computational Linguistics, 2021. doi: 10.18653/v1/2021.findings-acl.98.

Donald E Powers, Jill C Burstein, Martin Chodorow, Mary E Fowles, and Karen Kukich. Stumping e-rater: Challenging the validity of automated essay scoring. ETS Research Report Series, 2001 (1), 2001.

Donald E Powers, Jill C Burstein, Martin Chodorow, Mary E Fowles, and Karen Kukich. Stumping e-rater: challenging the validity of automated essay scoring. Computers in Human Behavior, 18 (2), 2002.

Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. OpenAI blog, 1(8), 2019.

Vikram Ramanarayanan, Klaus Zechner, and Keelan Evanini. Spoken language technology for language learning & assessment. http://www.interspeech2020.org/uploadfile/pdf/Tutorial-B-4.pdf, 2020.

Marco Túlio Ribeiro, Sameer Singh, and Carlos Guestrin. “why should I trust you?”: Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, August 13-17, 2016. ACM, 2016. doi: 10.1145/2939672.2939778.
Brian Riordan, Andrea Horbach, Aoife Cahill, Torsten Zesch, and Chong Min Lee. Investigating neural architectures for short answer scoring. In Proceedings of the 12th Workshop on Innovative Use of NLP for Building Educational Applications. Association for Computational Linguistics, 2017. doi: 10.18653/v1/W17-5017.

Jui Shah, Yaman Kumar Singla, Changyou Chen, and Rajiv Ratn Shah. What do audio transformer models hear? Probing acoustic representations for language delivery and its structure. arXiv preprint arXiv:2101.00387, 2021.

Avanti Shrikumar, Peyton Greenside, Anna Shcherbina, and Anshul Kundaje. Not just a black box: Learning important features through propagating activation differences. arXiv preprint arXiv:1605.01713, 2016.

Yaman Kumar Singla, Avykat Gupta, Shaurya Bagga, Changyou Chen, Balaji Krishnamurthy, and Rajiv Ratn Shah. Speaker-conditioned hierarchical modeling for automated speech scoring, 2021.

SLTI-SOPI. Ai-rated speaking exam for professionals (ai sopi). https://secondlanguagetesting.com/products-%26-services, 2021.

Tovia Smith. More states opting to 'robo-grade' student essays by computer. https://www.npr.org/2018/06/30/624373367/more-states-opting-to-robo-grade-student-essays-by-computer, 2018.

Mukund Sundararajan, Ankur Taly, and Qiqi Yan. Axiomatic attribution for deep networks. In Proceedings of the 34th International Conference on Machine Learning, ICML 2017, Sydney, NSW, Australia, 6-11 August 2017, volume 70 of Proceedings of Machine Learning Research. PMLR, 2017.

Kaveh Taghipour and Hwee Tou Ng. A neural approach to automated essay scoring. In Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing. Association for Computational Linguistics, 2016. doi: 10.18653/v1/D16-1193.

Yi Tay, Minh C. Phan, Luu Anh Tuan, and Siu Cheung Hui. Skipflow: Incorporating neural coherence features for end-to-end automatic text scoring. In Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, (AAAI-18), the 30th innovative Applications of Artificial Intelligence (IAAI-18), and the 8th AAAI Symposium on Educational Advances in Artificial Intelligence (EAAI-18), New Orleans, Louisiana, USA, February 2-7, 2018. AAAI Press, 2018.

Ian Tenney, Patrick Xia, Berlin Chen, Alex Wang, Adam Poliak, R. Thomas McCoy, Najoung Kim, Benjamin Van Durme, Samuel R. Bowman, Dipanjan Das, and Ellie Pavlick. What do you learn from context? probing for sentence structure in contextualized word representations. In 7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019. OpenReview.net, 2019.

USBE. Utah state board of education 2018–19 fingertip facts. https://www.ets.org/s/gre/pdf/gre_guide_table1a.pdf, 2020.

Eric Wallace, Shi Feng, Nikhil Kandpal, Matt Gardner, and Sameer Singh. Universal adversarial triggers for attacking and analyzing NLP. In Proceedings of the 2019 Conference on Empirical
Yucheng Wang, Zhongyu Wei, Yaqian Zhou, and Xuanjing Huang. Automatic essay scoring incorporating rating schema via reinforcement learning. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 2018. doi: 10.18653/v1/D18-1090.

James W Whitlock. *Automatic data processing in education*. Macmillan, 1964.

Duanli Yan, André A Rupp, and Peter W Foltz. *Handbook of automated scoring: Theory into practice*. CRC Press, 2020.

Su-Youn Yoon and Shasha Xie. Similarity-based non-scorable response detection for automated speech scoring. In *Proceedings of the Ninth Workshop on Innovative Use of NLP for Building Educational Applications*. Association for Computational Linguistics, 2014. doi: 10.3115/v1/W14-1814.

Su-Youn Yoon and Klaus Zechner. Combining human and automated scores for the improved assessment of non-native speech. *Speech Communication*, 93, 2017.

Su-Youn Yoon, Aoife Cahill, Anastassia Loukina, Klaus Zechner, Brian Riordan, and Nitin Madnani. Atypical inputs in educational applications. In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 3 (Industry Papers)*. Association for Computational Linguistics, 2018. doi: 10.18653/v1/N18-3008.

Zhou Yu, Vikram Ramanarayanan, David Suendermann-Oeft, Xinhao Wang, Klaus Zechner, Lei Chen, Jidong Tao, Aliaksei Ivanou, and Yao Qian. Using bidirectional lstm recurrent neural networks to learn high-level abstractions of sequential features for automated scoring of non-native spontaneous speech. In *2015 IEEE Workshop on Automatic Speech Recognition and Understanding (ASRU)*. IEEE, 2015.

Wei Emma Zhang, Quan Z Sheng, Ahoud Alhazmi, and Chenliang Li. Adversarial attacks on deep-learning models in natural language processing: A survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(3), 2020.

Siyuan Zhao, Yaqiong Zhang, Xiaolu Xiong, Anthony Botelho, and Neil Heffernan. A memory-augmented neural model for automated grading. In *Proceedings of the Fourth (2017) ACM Conference on Learning@ Scale*, 2017.

Xuhui Zhou, Yue Zhang, Leyang Cui, and Dandan Huang. Evaluating commonsense in pre-trained language models. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, 2020.
Appendices

8. Full Version of Abridged Main Paper Figures

The essays with their sentences shuffled are displayed in Figure 5. The full-size attribution images are given in Figures 9 to 12.

Figure 8: Attributions for SkipFlow and MANN respectively of an essay sample where all the sentences have been randomly shuffled. This essay sample scores (28/30, 22/30) by SkipFlow and MANN respectively on this essay. The original essay also scored (28/30) and (22/30) respectively.

9. Statistics: Iterative Addition of Words

The results are given in table 8.

| %  | $\mu_{pos}$ | $\mu_{neg}$ | $N_{pos}$ | $N_{neg}$ | $\sigma$ |
|----|-------------|-------------|----------|----------|---------|
| 80 | 3.5/1.1/0.002 | 0.43/0.09/0.05 | 65/31/0.63 | 8.9/2.88/91.6 | 5.1/2/0.06 |
| 60 | 4/0.37/0.001 | 1.01/1.4/0.14 | 60/9.2/0.3 | 17/39.1/99 | 6.7/2.6/0.14 |
| 40 | 3/0.07/0 | 3.7/5.8/0.23 | 36/2.24/0 | 44/88.4/99.6 | 9.24/6/5.0/24 |
| 20 | 2.09/0.02/0.002 | 14/7/13.7/0.31 | 15.6/0.6/0.63 | 78.5/94.5/99.3 | 19.5/14/5.32 |
| 0 | 61/0/0 | 0/20/0 | 0/0/0 | 100/94.5/100 | 62/22.3/0.5 |

Table 8: Statistics for iterative addition of the most-attributed words on Prompt 7. Legend (Kumar et al. 2020): { epile: % words added to form a response, $\mu_{pos}$: Mean difference of positively impacted samples (as % of score range), $\mu_{neg}$: Mean difference of negatively impacted samples (as % of score range), $N_{pos}$: Percentage of positively impacted samples, $N_{neg}$: Percentage of negatively impacted samples, $\sigma$: Standard deviation of the difference (as % of score range)}

10. Statistics: Iterative Removal of Words

11. BERT-model Hyperparameters
Figure 9: Full-Sized Attributions for SkipFlow, MANN and BERT respectively of an essay sample where all the sentences have been randomly shuffled.

Table 9: Statistics for iterative removal of least attributed words on Prompt 7. Legend (Kumar et al., 2020): (%: % words removed from a response, $\mu_{pos}$: Mean difference of positively impacted samples (as % of score range), $\mu_{neg}$: Mean difference of negatively impacted samples (as % of score range), $N_{pos}$: Percentage of positively impacted samples, $N_{neg}$: Percentage of negatively impacted samples)
patience has not and in all forever will be in the way we are the most of some of and others on the family lies in the of along with the field of why is done so to the reply to this it that in my I I have learned of my class will always the same two different to receive rays at the almost on the for the only thing it also the ray to by family because many of the of those involved too on the understanding changes which is that but a house frequently of the should be the more a and the the less for the same brain will different with to gain our personal at the we is can be but not in my class many of the by personal on the we of a of house might be the of my also state of to a not the our personal with the we is yet another but at understanding changes understanding which will be the and for the often by a understanding because are on those in question of family also at will always be an experience of in my of class none of the to our personal with the we most of the but even so knowing that the that the should be an many of the for my that by the in my class almost all of the the to our personal on the we an those in question of for me is not our personal with the we the on the sooner a or the more that be a can be has not and never will be and with the that of the of the personal with the we become of me can become patience will always be an experience of because of the fact that family by the for which on human life should immediately

Figure 10: Full-Sized Attributions for SkipFlow, MANN and BERT respectively of an BABEL essay sample.
Figure 11: Full-Sized Attributions for SkipFlow, MANN and BERT respectively of an essay sample where all the sentences have an added false fact.

| HyperParameter       | Value                  |
|----------------------|------------------------|
| Optimizer            | Adam                   |
| Learning Rate        | 2e-5                   |
| Batch Size           | 8                      |
| Epochs               | 5-10 based on Early Stopping |
| Loss                 | Mean Squared Error     |

Table 10: Bert Model Hyperparameters and Architecture
Figure 12: Full-Sized Attributions for SkipFlow, MANN and BERT respectively of a real essay sample.