TextFlint: Unified Multilingual Robustness Evaluation Toolkit for Natural Language Processing

Xiao Wang, Qin Liu, Tao Gui, Qi Zhang, Yicheng Zou, Xin Zhou, Jiacheng Ye, Yongxin Zhang, Rui Zheng, Zexiong Pang, Qinzhuo Wu, Zhengyan Li, Chong Zhang, Ruotian Ma, Zichu Fei, Rujian Cai, Jun Zhao, Xingwu Hu, Zhiheng Yan, Yiding Tan, Yuan Hu, Qiuyuan Bian, Zhihua Liu, Shan Qiu, Bolin Zhu, Xiaooyu Xing, Jinlan Fu, Yue Zhang, Minlong Peng, Xiaojing Huang

School of Computer Science, Fudan University

{xiao.wang20, liuq19, tgui16, qz}@fudan.edu.cn

Abstract

TextFlint is a multilingual robustness evaluation toolkit for NLP tasks that incorporates universal text transformation, task-specific transformation, adversarial attack, subpopulation, and their combinations to provide comprehensive robustness analysis. This enables practitioners to automatically evaluate their models from various aspects or to customize their evaluations as desired with just a few lines of code. TextFlint also generates complete analytical reports as well as targeted augmented data to address the shortcomings of the model in terms of its robustness. To guarantee acceptability, all the text transformations are linguistically based and all the transformed data (up to 100,000 texts) passed human evaluation. To validate the utility, we performed large-scale empirical evaluations (over 67,000) on state-of-the-art deep learning models, classic supervised methods, and real-world systems. The toolkit is already available at https://github.com/textflint, with all the evaluation results demonstrated at textflint.io.

1 Introduction

The detection of model robustness is attracting increasing attention in recent years, given that deep neural networks (DNNs) of high accuracy can still be vulnerable to carefully crafted adversarial examples (Li et al., 2020), distribution shift (Miller et al., 2020), data transformation (Xing et al., 2020), and shortcut learning (Geirhos et al., 2020). Existing approaches to textual robustness evaluation focus on slightly modifying the input data, which maintains the original meaning and results in a different prediction. However, these methods often concentrate on either universal or task-specific generalization capabilities, which is difficult to make a comprehensive evaluation.

In response to the shortcomings of recent works, we introduce TextFlint, a unified, multilingual, and analyzable robustness evaluation toolkit for NLP. Its features include:

1. Integrity. TextFlint offers 20 general transformations and 60 task-specific transformations, as well as thousands of their combinations, which cover a variety of aspects of text transformations to enable comprehensive evaluation of robustness. It also supports evaluations in multiple languages. In addition, the toolkit also incorporates adversarial attack and subpopulation (Figure 1).

2. Acceptability. All the text transformations offered by TextFlint are linguistically based and...
Figure 2: Architecture of TextFlint. Input Layer receives the original dataset, config file and target model as input, which are represented as Dataset, Config and FlintModel separately. Generation Layer consists of three parallel modules, where Subpopulation generates a subset of input dataset, Transformation augments datasets, and AttackRecipe interacts with the target model. Report Layer analyzes test results by Analyzer and provides users with robustness report by ReportGenerator.

passed human evaluation. To verify the quality of the transformed text, we conducted human evaluation on the original and transformed texts under all of the mentioned transformations. The transformed texts perform well in plausibility and grammaticality.

3. **Analyzability.** Based on the evaluation results, TextFlint provides a standard analysis report with respect to a model’s lexics, syntax, and semantics. All the evaluation results can be displayed via visualization and tabulation to help users gain a quick and accurate grasp of the shortcomings of a model. In addition, TextFlint generates a large number of targeted data to augment the evaluated model, based on the the defects identified in the analysis report, and provides patches for the model defects.

We evaluated 95 state-of-the-art models and classic systems on 6,903 transformation datasets for a total of over 67,000 evaluations and found almost all models showed significant performance degradation, including a decline of more than 50% of BERT’s prediction accuracy on tasks such as aspect-level sentiment classification, named entity recognition, and natural language inference. This means that the robustness of most models need to be improved.

2  **TextFlint Framework**

TextFlint is designed to be flexible enough to allow practitioners to configure the workflow while providing appropriate abstractions to alleviate the concerns of the low-level implementation. According to its pipeline architecture, it can be organized into three blocks, as shown in Figure 2: (a) Input Layer, which prepares necessary information for sample generation; (b) Generation Layer, which applies generation functions to each sample; and (c) Reporter Layer, which analyzes the evaluation results and generates a robustness report.

2.1 **Input Layer**

For input preparation, the original dataset, which is to be loaded by Dataset, should first be formatted as a series of JSON objects. The configuration of TextFlint is specified by Config, which can be loaded from a customized config file. The target model is wrapped by FlintModel, which needs to implement certain interfaces to support specific functions. After Input Layer completes the required input loading, the interaction between TextFlint and the user is complete.

2.2 **Generation Layer**

Generation Layer supports three types of sample generation functions to provide comprehensive
robustness analysis, i.e., Transformation, Subpopulation, and AttackRecipe. It is worth noting that the procedure of Transformation and Subpopulation does not require querying the target model, which means it is a completely decoupled process with the target model prediction. Besides, to ensure semantic and grammatical correctness of transformed samples, Validator provides several metrics to calculate confidence of each sample.

**Transformation** Transformation aims to generate perturbations of the input text while maintaining the acceptability of transformed texts. In order to verify the robustness comprehensively, TextFlint offers 20 universal transformations and 60 task-specific transformations, as well as thousands of their combinations, covering 12 NLP tasks.

From the perspective of linguistics, the transformations are designed according to morphology, syntax, paradigmatic relation, and pragmatics. Transformations on morphology includes **Key-Board**, **Ocr**, **Typos**, etc. As for syntactical transformations, there are **SwapSyn-WordNet**, **AddSubTree**, etc. Due to limited space, refer to Figure 3 for specific information. Besides, we conducted a large scale human evaluation on the original and transformed texts under all of the mentioned transformations (Section 4).

**Subpopulation** Subpopulation identifies the specific part of the dataset on which the target model performs poorly. To retrieve a subset that meets the configuration, Subpopulation divides the dataset through sorting samples by certain attributes. TextFlint provides four general Subpopulation configurations, which contains **GenderBias**, **TextLength**, **LanguageModelPerplexity**, and **PhraseMatching**, which work for most NLP tasks. Take the configuration of text length for example, Subpopulation retrieves the subset of the top 20% or bottom 20% in length.

**AttackRecipe** AttackRecipe aims to find a perturbation of an input text satisfies the goal to fool the given FlintModel. In contrast with Transformation and Subpopulation, AttackRecipe requires the prediction scores of the target model. TextFlint provides 16 easy-to-use adversarial attack recipes which are implemented based on TextAttack (Morris et al., 2020).

### 2.3 Reporter Layer

Generation Layer yields three types of adversarial samples and verifies the robustness of the target model. Based on the evaluation results from Generation Layer, Report Layer aims to provide users with a standard analysis report from syntax, morphology, pragmatics, and paradigmatic relation aspects. The running process of Report Layer can be regarded as a pipeline from Analyzer to ReportGenerator.
3 Usage

Using TextFlint to verify the robustness of a specific model is as simple as running the following command:

```
$ textflint --dataset input_file --config config.json
```

where `input_file` is the input file of csv or json format, `config.json` is a configuration file with generation and target model options. Complex functions can be implemented by a simple modification on `config.json`, such as executing the pipeline of transformations and assigning the parameters of each transformation method. Take the configuration for TextCNN (Kim, 2014) model on SA (sentiment analysis) task as example:

```json
{
  "task": "SA",
  "out_dir": "/DATA/",
  "flint_model": "/textcnn_model.py",
  "trans_methods": [
    "Ocr",
    ["InsertAdv", "SwapNamedEnt"],
    ...
  ],
  "trans_config": {
    "Ocr": {"trans_p": 0.3},
    ...
  }
}
```

- **task** is the name of target task. TextFlint supports 12 types of tasks.
- **out_dir** is the directory where each of the generated sample and its corresponding original sample are saved.
- **flint_model** is the python file path that saves the instance of FlintModel.
- **trans_methods** is used to specify the transformation method. For example, "Ocr" denotes the universal transformation Ocr, and ["InsertAdv", "SwapNamedEnt"] denotes a pipeline of task-specific transformations, namely InsertAdv and SwapNamedEnt.
- **trans_config** configures the parameters for the transformation methods. The default parameter is also a good choice.

Moreover, it also supports the configuration of subpopulation and adversarial attack. For more details about parameter configuration, please move to [https://github.com/textflint/textflint](https://github.com/textflint/textflint).

Based on the design of decoupling sample generation and model verification, TextFlint can be used inside another NLP project with just a few lines of code.

```python
from textflint import Engine
data_path = 'input_file'
cfg = 'config.json'
engine = Engine()
extrack = engine.run(data_path, config)
```

TextFlint is also available for use through our web demo, displayed in Figure 4, which is available at [https://www.textflint.io/demo](https://www.textflint.io/demo).

Case Studies of Usage Due its user-friendly design philosophy, TextFlint shows its practicality in real application. We summarize three occasions in which users would find challenging in model robustness evaluation:

**Case 1: General Evaluation** For users who want to evaluate robustness of NLP models in a general way, TextFlint supports generating massive and comprehensive transformed samples within one command. By default, TextFlint performs all single transformations on the original dataset to form corresponding transformed datasets, and the performance of target models is tested on these datasets. The evaluation report provides a comparative view of model performance on datasets before and after certain types of transformation, which supports model weakness analysis and guides particular improvement. For example, take BERT base (Devlin et al., 2019) as the target model to verify its robustness on the CONLL2003...
Table 1: Human evaluation results for task-specific transformation. Ori and Trans denote the original text and the transformed text, respectively. The table on the left is the performance of task-specific transformations for the sentiment analysis task, and the right is of that for named entity recognition. These metrics are rated on a 1-5 scale (5 denotes the best).

<table>
<thead>
<tr>
<th>Morphology</th>
<th>ParadigmaticRelation</th>
<th>Other</th>
<th>Pragmatics</th>
<th>Syntax</th>
<th>SwapSyn</th>
<th>Case</th>
<th>Number</th>
<th>Twitter</th>
<th>AppendIrr</th>
<th>Punctuation</th>
<th>InsertAdv</th>
<th>0.6</th>
<th>0.7</th>
<th>0.8</th>
<th>0.9</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ori.</strong></td>
<td><strong>Trans.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>DoubleDenial</strong></td>
<td>3.26</td>
<td>3.37</td>
<td>3.59</td>
<td>3.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>AddSum-Person</strong></td>
<td>3.39</td>
<td>3.32</td>
<td>3.76</td>
<td>3.59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>AddSum-Movie</strong></td>
<td>3.26</td>
<td>3.34</td>
<td>3.61</td>
<td>3.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>SwapSpecialEnt-Person</strong></td>
<td>3.37</td>
<td>3.14</td>
<td>3.75</td>
<td>3.73</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>SwapSpecialEnt-Movie</strong></td>
<td>3.17</td>
<td>3.28</td>
<td>3.70</td>
<td>3.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>OOV</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.69</td>
<td>3.76</td>
<td>3.54</td>
<td>3.48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>SwapLonger</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.73</td>
<td>3.66</td>
<td>3.77</td>
<td>3.54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>EntTypos</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.57</td>
<td>3.5</td>
<td>3.59</td>
<td>3.54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>CrossCategory</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.48</td>
<td>3.44</td>
<td>3.41</td>
<td>3.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
<tr>
<td><strong>ConcatSent</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4.14</td>
<td>3.54</td>
<td>3.84</td>
<td>3.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>---</td>
</tr>
</tbody>
</table>

Figure 5: Robustness report of BERT base model on CONLL2003 dataset, where trans_f1 denotes the F1-score of target model on the transformed test data.

Performance would provide concrete suggestions on model improvement. By using TextFlint and applying a transformed dataset to target models, the transformations corresponding to significant performance decline in the evaluation report will provide improvement guidance of target models. Moreover, TextFlint supports adversarial training on target models with a large-scale transformed dataset, and the change of performance will also be reported to display performance gain due to adversarial training.

4 Benchmarking Existing Models with TextFlint

To verify the quality of transformation, we conduct human evaluation on the original and transformed texts under all of the mentioned transformations. Specifically, we consider two metrics in human evaluation: plausibility and grammaticality. For each of the transformed text, three native speakers from Amazon Mechanical Turk are invited for evaluation and the average score is recorded. All of the 100,000 texts pass human evaluation in terms of the two metrics. It is verified that the plausibility and grammaticality of transformed texts, take the data of SA and NER for example (Table 1), only drop slightly compared with the original ones.

We adopt TextFlint to evaluate hundreds of models of 12 tasks (including tasks on Chinese), covering various model frameworks and learning schemas, ranging from traditional feature-based machine learning approaches to state-of-the-art neural networks. All evaluated models and their implementations are available publicly. After model implementation, dataset transformation, and batch inspection, users will receive evaluation reports on various aspects, comprehensively analyzing the robustness of a system by acquiring larger test samples. From the evaluation reports, we can
easily compare the model results of the original test set with those of the transformed set, spotting the main defects of the input model and identifying the model that performs the best or worst.

From the numerous evaluations and comparisons conducted by TextFlint, we have a thorough view of existing NLP systems and discover underlying patterns about model robustness. As for the ABSA task (Table 2), methods equipped with pre-training LMs show better performance than other models on the task-specific transformations, e.g., AddDiff, where the accuracy score of BERT-Aspect drops from 90.32 to merely 81.58. All the evaluation results and comprehensive robustness analysis are available at textflint.io.

5 Related Work

Our work is related to many existing open-source tools and works in different areas.

Robustness Evaluation Many tools include evaluation methods for robustness, including NLPAug (Ma, 2019), Errudite (Wu et al., 2019), AllenNLP Interpret (Wallace et al., 2019), and Checklist (Ribeiro et al., 2020), which are only applicable to limited parts of robustness evaluations, while TextFlint supports comprehensive evaluation methods, e.g., subpopulation, adversarial attacks, transformations, and so on.

Several tools also exist concerning robustness, which are similar to our work (Morris et al., 2020; Zeng et al., 2020; Goel et al., 2021) and include a wide range of evaluation methods. However, these tools only focus on general generalization evaluations and lack quality evaluations on generated texts or only support automatic quality constraints. TextFlint supports both general and task-specific evaluations and guarantees the acceptability of each transformation method with human evaluations. Additionally, TextFlint provides a standard report that can be displayed with visualization and tabulation.

Interpretability and Error Analysis Several works concern model evaluation from different perspectives. AllenNLP Interpret (Wallace et al., 2019), InterpretreML (Nori et al., 2019), LIT (Nori et al., 2019), Manifold (Zhang et al., 2018), and AIX360 (Arya et al., 2019) care about model interpretability, attempting to understand the models’ behavior through different evaluation methods. CrossCheck (Arendt et al., 2020), AllenNLP Interpret (Wallace et al., 2019), Errudite (Wu et al., 2019), and Manifold (Zhang et al., 2018) offer visualization and cross-model comparison for error analysis. TextFlint is differently motivated yet complementary with these works, which can provide comprehensive analysis on models’ defects, thus contributing to better model understanding.

6 Conclusion

We introduce TextFlint, a unified multilingual robustness evaluation toolkit that incorporates universal text transformation, task-specific transformation, adversarial attack, subpopulation, and their combinations to provide comprehensive robustness analysis. TextFlint enables practitioners to evaluate their models with just a few lines of code and then obtain complete analytical reports. We performed large-scale empirical evaluations on state-of-the-art deep learning models, classic supervised methods, and real-world systems. Almost all models showed significant performance degradation, indicating the urgency and necessity of including robustness into NLP model evaluations.
Ethical Considerations

For the consideration of ethical concerns, we would make detailed description as following:

1. All of the transformed data comes from existing datasets, which are derived from public scientific papers. Due to the limited space, we detail the characteristics of the dataset and the transformation methods in the README.md file at https://github.com/textflint/textflint.

2. The quality of the transformed datasets will affect the credibility of the robustness evaluation. Compared with previous work, we additionally evaluated 100,000 samples from all of the transformation methods with respect to their plausibility and grammaticality by human evaluation.

3. TextFlint is a robustness evaluation toolkit, which does not provide any NLP models for specific tasks, such as automated essay scoring, hate speech, and so on. Therefore, there is no potential harm to vulnerable populations.

4. Our work does not contain identity characteristics. It does not harm anyone.

5. The subpopulation and transformation modules are executed on the CPU and do not consume a lot of computing resources. The AttackRecipe module is implemented based on TextAttack (Morris et al., 2020), which is a widely used framework for adversarial attacks and does not cause excessive computational cost.

References


