- 004
- 005

- 008

- 012

014

015

016

017

018

019

020

021

022

023

024

025

026

027

028

029

030

031

032

033

034

035

036

037

038

039

040

041

042

043

044

045

046

047

048

049

- 006
- 007
- 009
- 010

# 011

- 013

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. 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 realworld systems. The toolkit is already available at https://github.com/textflint, with all the eval-

Abstract

#### 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

uation results demonstrated at textflint.io.

# Transformation

Original	Tasty burgers, and crispy fries. (Target a	spect: burgers)			
RevTgt	Terrible burgers, but crispy fries.				
RevNon	Tasty <b>burgers</b> , but soggy fries.				
Typos Tatsy burgers, and cripsy fries.					
Adver	sarial attack				
Original	Premise: Some rooms have balconies. Hypothesis: All of the rooms have balcor	nies. Contradiction			
Adv	Premise: Many rooms have balconies. Hypothesis: All of the rooms have balcon	nies. Neutral			
Subpo	pulation				
Original	Set Su	bpopulation - Gender			
She beca	me a nurse and worked in a hospital.	$\checkmark$			
I told Joh	n to come early, but he failed.	$\checkmark$			
The river	derives from southern America.	X			
Marry wo	ould like to teach kids in the kindergarten.	$\checkmark$			
The storn	n destroyed many houses in the village.	X			

050

051

052

053

054

055

056

057

058

059

060

061

062

063

064

065

066

067

068

069

070

071

072

073

074

075

076

077

078

079

080

081

082

083

084

085

086

087

088

089

090

091

092

093

094

095

096

097

098

099

Figure 1: Examples of three main generation functions. The example of transformation is from ABSA (Aspectbased Sentiment Analysis) task, where the italic bold RevTgt (short for reverse target) denotes task-specific transformations and the bold Typos denotes universal

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

**TextFlint:** Unified Multilingual Robustness Evaluation Toolkit for

**Natural Language Processing** 

Xiao Wang<sup>\*</sup>, Oin Liu<sup>\*</sup>, Tao Gui<sup>†</sup>, Oi Zhang<sup>†</sup>, Yicheng Zou, Xin Zhou,

Jiacheng Ye, Yongxin Zhang, Rui Zheng, Zexiong Pang, Qinzhuo Wu,

Zhengyan Li, Chong Zhang, Ruotian Ma, Zichu Fei, Ruijian Cai, Jun Zhao,

Xingwu Hu, Zhiheng Yan, Yiding Tan, Yuan Hu, Qiyuan Bian, Zhihua Liu,

Shan Qin, Bolin Zhu, Xiaoyu Xing, Jinlan Fu, Yue Zhang, Minlong Peng,

Xiaoqing Zheng, Yaqian Zhou, Zhongyu Wei, Xipeng Qiu and Xuanjing Huang

School of Computer Science, Fudan University

{xiao\_wang20, liug19, tgui16, gz}@fudan.edu.cn

# This enables

transformation.

<sup>\*</sup>Xiao Wang and Qin Liu contributed equally to this work and are co-first authors.

<sup>&</sup>lt;sup>†</sup>Corresponding Author

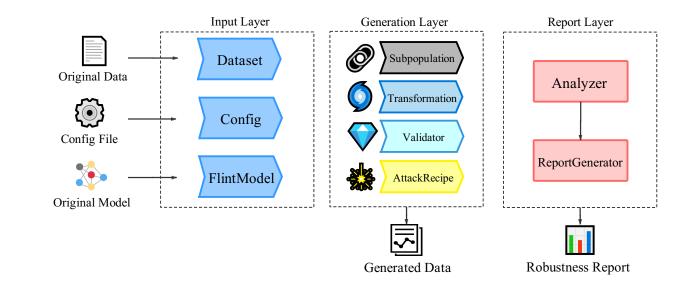


Figure 2: Architecture of TextFlint. Input Layer receives the original dataset, config file and target model as input, which are represented as Dataset, Config and FlintModel separately. Generation Layer consists of three parallel modules, where Subpopulation generates a subset of input dataset, Transformation 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

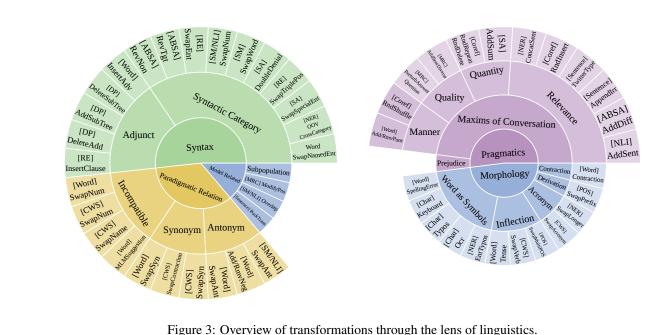
TextFlint is designed to be flexible enough to allow practitioners to configure the workflow while providing appropriate abstractions to alleviate the concerns of the low-level implementation. According to its pipeline architecture, it can be organized into three blocks, as shown in Figure 2: (a) Input 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 trans-formations 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. То 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

300

301

302

303

304

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

344

345

346

347

348

349

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

305 <sup>1</sup> <sup>\$</sup> 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:

```
1
     "task": "SA",
2
     "out_dir": "./DATA/",
3
     "flint_model": "./textcnn_model.py",
4
5
     "trans_methods": [
6
       "Ocr"
       ["InsertAdv", "SwapNamedEnt"],
7
8
9
10
     "trans_config": {
       "Ocr": {"trans_p": 0.3},
11
12
13
     },
14
   . . .
15
```

- 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.
- 337 • trans\_methods is used to specify the 338 transformation method. For example, "Ocr" 339 denotes the universal transformation Ocr, and 340 ["InsertAdv", "SwapNamedEnt"] 341 denotes а pipeline of task-specific transformations, *InsertAdv* namely and 342 SwapNamedEnt. 343
  - 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

TextFlint		350
Task ABSA •	Transformed Data	351
	Result 0	352
Transformation	ori: The bread is top notch as well.	
Ocr +	trans: The bread is t0p notch as well.	353
Sample	Result 1	354
Enter the original data	ori: I have to say they have one of the fastest delivery times in the city.	355
	trans: I have to 8ay they have une of the fastest delivery time8 in the city.	356
Submit		357
	Result 2	358
	ori: Food is always fresh and hot ready to eat!	550
	trans: Fo0d is alway8 fresh and hot ready to eat!	359
	Result 3	360
	ori: Did I mention that the coffee is OUTSTANDING?	361
	trans: Did I mention that the cuffee is OUTSTANDING?	301
		362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

Figure 4: Screenshot of TextFlint's web interface running Ocr transformation for ABSA task.

details about parameter configuration, please move to 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.

from textflint import Engine
data\_path = 'input\_file'
config = 'config.json'

```
engine = Engine()
```

2

3

4

5

6

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.

**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

400		Plaus	sibility	Gram	naticality		Plau	sibility	Gram	naticality
401		Ori.	Trans.	Ori.	Trans.		Ori.	Trans.	Ori.	Trans.
402	DoubleDenial	3.26	3.37	3.59	3.49	OOV	3.69	3.76	3.54	3.48
403	AddSum-Person	3.39	3.32	3.76	3.59	SwapLonger	3.73	3.66	3.77	3.54
404	AddSum-Movie	3.26	3.34	3.61	3.58	EntTypos	3.57	3.5	3.59	3.54
	SwapSpecialEnt-Person	3.37	3.14	3.75	3.73	CrossCategory	3.48	3.44	3.41	3.32
405	SwapSpecialEnt-Movie	3.17	3.28	3.70	3.49	ConcatSent	4.14	3.54	3.84	3.81
406										

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).

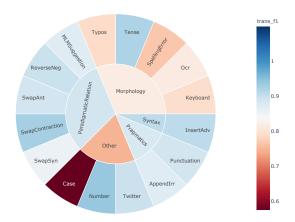


Figure 5: Robustness report of BERT base model on CONLL2003 dataset, where trans\_f1 denotes the F1-score of target model on the transformed test data.

dataset(Tjong Kim Sang and De Meulder, 2003), its robustness report is shown in Figure 5.

*Case 2: Customized Evaluation* For users who want to test model performance on specific aspects, they demand a customized transformed dataset of certain transformations or their combinations. In TextFlint, this could be achieved by modifying Config, which determines the configuration of TextFlint in generation. Config specifies the transformations being performed on the given dataset, and it could be modified manually or generated automatically. Through modifying the configuration, users could decide to generate multiple transformed samples on each original data sample, validate samples by semantics, preprocess samples with certain processors, etc.

*Case 3: Target Model Improvement* For users who want to improve robustness of target models, they may work hard to inspect the weakness of model with less alternative support. To tackle the issue, we believe a diagnostic report revealing the influence of comprehensive aspects on model 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

#### ACL-IJCNLP 2021 Submission \*\*\*. Confidential Review Copy. DO NOT DISTRIBUTE.

$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	Model	RevTgt (Or	i. $\rightarrow$ Trans.)	<i>RevNon</i> (Ori. $\rightarrow$ Trans.)		AddDiff (Ori. $\rightarrow$ Trans.)		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	Model	Accuracy	Macro-F1	Accuracy	Macro-F1	Accuracy	Macro-F1	
$ \begin{array}{c} \text{TD-LSTM} \ (\text{Tang et al., 2016a}) \\ \text{ATAE-LSTM} \ (\text{Wang et al., 2016b}) \\ \text{MemNet} \ (\text{Tang et al., 2017b}) \\ \text{MemNet} \ (\text{Li et al., 2017b}) \\ \text{MemNet} \ (\text{Li et al., 2017b}) \\ \text{MemNet} \ (\text{Li et al., 2018b}) \\ \text{MGAN} \ (\text{Fan et al., 2018b}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019b}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019b}) \\ \text{BERT+aspect} \ (\text{Devlin et al., 2019b}) \\ \text{MemNet} \ (\text{Zeng et al., 2019b}) \\ \text{MemNet} \ $	Restaurant Dataset							
$ \begin{array}{c} \text{ATAE-LSTM} \ (\text{Wang et al., 2016}) \\ \text{MemNet} \ (\text{Tang et al., 2016}) \\ \text{MemNet} \ (\text{Tang et al., 2016b}) \\ \text{MemNet} \ (\text{Tang et al., 2016b}) \\ \text{ATAE-LSTM} \ (\text{Wang et al., 2016b}) \\ \text{MemNet} \ (\text{Tang et al., 2016b}) \\ \text{ATAE-LSTM} \ (\text{Wang et al., 2016b}) \\ \text{Attage to al., 2017}) \\ \text{Attage tal., 2017} \\ \text{Attage tal., 2017} \\ \text{Attage tal., 2017} \\ \text{TNet} \ (\text{Li et al., 2018}) \\ \text{MGAN} \ (\text{Fan et al., 2018}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019}) \\ \text{BERT+aspect} \ (\text{Devlin et al., 2019}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019}) \\ \text{BERT-base} \ (\text{Devlin et al., 2019}) \\ \text{BALL} \ \text{Attage tal., 2019} \\ \text{BALL} \ \text{Attage tal., 2019} \\ Attage tal.,$	LSTM (Hochreiter et al., 1997)	$84.42 \rightarrow 19.30$	55.75  ightarrow 19.88	$85.91 \rightarrow 73.42$	$55.02 \rightarrow 44.69$	$84.42 \rightarrow 44.63$	55.75  ightarrow 33.24	
	TD-LSTM (Tang et al., 2016a)	$86.42 \rightarrow 22.42$	$61.92 \rightarrow 22.28$	$87.29 \rightarrow 79.58$	$60.70 \rightarrow 53.35$	$84.42 \rightarrow 81.35$	$61.92 \rightarrow 55.69$	
$ \begin{array}{c} \text{IAN (Ma et al., 2017)} \\ \text{TNet (Li et al., 2018)} \\ \text{MGAN (Fan et al., 2018)} \\ \text{BERT-base (Devlin et al., 2019)} \\ \text{BERT+aspect (Devlin et al., 2019)} \\ \text{Devlin et al., 2019} \\ Devlin et a$	ATAE-LSTM (Wang et al., 2016)	$85.60 \rightarrow 28.90$	$67.02 \rightarrow 23.84$	$86.60 \rightarrow 60.74$	$65.41 \rightarrow 41.46$	$85.60 \rightarrow 44.39$	$67.02 \rightarrow 36.40$	
$ \begin{array}{c} \text{TNet} \ (\text{Li et al.}, 2018) \\ \text{MGAN} \ (\text{Fan et al.}, 2018) \\ \text{BERT-base} \ (\text{Devlin et al.}, 2019) \\ \text{BERT+aspect} \ (\text{Devlin et al.}, 2019) \\ \text{LCF-BERT} \ (\text{Zeng et al.}, 2019) \\ \end{array} \\ \begin{array}{c} 87.37 \rightarrow 24.58 \\ 87.37 \rightarrow 24.58 \\ 86.629 \rightarrow 25.00 \\ 69.98 \rightarrow 23.65 \\ 90.8 \rightarrow 23.65 \\ 90.55 \rightarrow 52.46 \\ 91.41 \rightarrow 57.04 \\ 77.53 \rightarrow 44.43 \\ 90.32 \rightarrow 81.58 \\ 76.56 \rightarrow 39.52 \\ 90.55 \rightarrow 61.09 \\ 75.18 \rightarrow 44.87 \\ 90.32 \rightarrow 86.78 \\ 76.56 \rightarrow 73.71 \\ \end{array} \\ \begin{array}{c} 87.37 \rightarrow 80.56 \\ 66.29 \rightarrow 59.68 \\ 69.98 \rightarrow 51.71 \\ 69.98 \rightarrow 51.71 \\ 70.66 \rightarrow 30.38 \\ 90.55 \rightarrow 52.46 \\ 71.45 \rightarrow 32.47 \\ 77.53 \rightarrow 44.43 \\ 90.32 \rightarrow 81.58 \\ 76.91 \rightarrow 71.01 \\ 90.32 \rightarrow 53.48 \\ 76.56 \rightarrow 39.52 \\ 90.55 \rightarrow 61.09 \\ 75.18 \rightarrow 44.87 \\ 90.32 \rightarrow 86.78 \\ 76.56 \rightarrow 73.71 \\ \end{array}$	MemNet (Tang et al., 2016b)	$81.46 \rightarrow 19.30$	54.57  ightarrow 17.77	$83.68 \rightarrow 72.95$	$55.39 \rightarrow 45.14$	$81.46 \rightarrow 63.62$	54.57  ightarrow 39.36	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	IAN (Ma et al., 2017)	$83.83 \rightarrow 17.71$	$58.91 \rightarrow 18.12$	$84.88 \rightarrow 73.06$	$56.91 \rightarrow 45.87$	$83.83 \rightarrow 56.61$	$58.91 \rightarrow 37.08$	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	TNet (Li et al., 2018)	87.37  ightarrow 24.58	$66.29 \rightarrow 25.00$	$87.86 \rightarrow 75.00$	$66.15 \rightarrow 49.09$	$87.37 \rightarrow 80.56$	$66.29 \rightarrow 59.68$	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	MGAN (Fan et al., 2018)	$88.15 \rightarrow 26.10$	$69.98 \rightarrow 23.65$	$89.06 \rightarrow 71.95$	$68.90 \rightarrow 50.24$	$88.15 \rightarrow 70.21$	$69.98 \rightarrow 51.71$	
LCF-BERT (Zeng et al., 2019) 90.32 $\rightarrow$ 53.48 76.56 $\rightarrow$ 39.52 90.55 $\rightarrow$ 61.09 75.18 $\rightarrow$ 44.87 90.32 $\rightarrow$ 86.78 76.56 $\rightarrow$ 73.71	BERT-base (Devlin et al., 2019)	$90.44 \rightarrow 37.17$	70.66  ightarrow 30.38	$90.55 \rightarrow 52.46$	$71.45 \rightarrow 32.47$	$90.44 \rightarrow 55.96$	$70.66 \rightarrow 37.00$	
	BERT+aspect (Devlin et al., 2019)	90.32  ightarrow 62.59	$76.91 \rightarrow 44.83$	$91.41 \rightarrow 57.04$	$77.53 \rightarrow 44.43$	$90.32 \rightarrow 81.58$	$76.91 \rightarrow 71.01$	
Average $86.83 \rightarrow 31.16$ $65.86 \rightarrow 26.63$ $87.78 \rightarrow 67.73$ $64.96 \rightarrow 45.15$ $86.83 \rightarrow 66.55$ $65.86 \rightarrow 49.49$	LCF-BERT (Zeng et al., 2019)	$90.32 \rightarrow 53.48$	76.56  ightarrow 39.52	$90.55 \rightarrow 61.09$	75.18  ightarrow 44.87	$90.32 \rightarrow 86.78$	$76.56 \rightarrow 73.71$	
	Average	$86.83 \rightarrow 31.16$	$65.86 \rightarrow 26.63$	$87.78 \rightarrow 67.73$	$64.96 \rightarrow 45.15$	$86.83 \rightarrow 66.55$	$65.86 \rightarrow 49.49$	

Table 2: Accuracy and F1 score on the SemEval 2014 Restaurant dataset.

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**

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

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.

560

561 562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

**Interpretability and Error Analysis** Several works concern model evaluation from different perspectives. AllenNLP Interpret (Wallace et al., 2019), InterpreteML (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 CrossCheck (Arendt et al., 2020), methods. 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.

#### Conclusion 6

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.

6

## Ethical Considerations

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

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

- Dustin Arendt, Zhuanyi Huang, Prasha Shrestha, Ellyn Ayton, Maria Glenski, and Svitlana Volkova. 2020. Crosscheck: Rapid, reproducible, and interpretable model evaluation.
- Vijay Arya, Rachel KE Bellamy, Pin-Yu Chen, Amit Dhurandhar, Michael Hind, Samuel C Hoffman, Stephanie Houde, Q Vera Liao, Ronny Luss, Aleksandra Mojsilović, et al. 2019. One explanation does not fit all: A toolkit and taxonomy of ai explainability techniques. *arXiv preprint arXiv:1909.03012*.
- Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. Bert: Pre-training of deep bidirectional transformers for language understanding. In Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers), pages 4171–4186.
  - Feifan Fan, Yansong Feng, and Dongyan Zhao. 2018. Multi-grained attention network for aspect-level

sentiment classification. In *Proceedings of the* 2018 conference on empirical methods in natural language processing, pages 3433–3442.

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

- Robert Geirhos, Jörn-Henrik Jacobsen, Claudio Michaelis, Richard Zemel, Wieland Brendel, Matthias Bethge, and Felix A Wichmann. 2020. Shortcut learning in deep neural networks. *Nature Machine Intelligence*, 2(11):665–673.
- Karan Goel, Nazneen Rajani, Jesse Vig, Samson Tan, Jason Wu, Stephan Zheng, Caiming Xiong, Mohit Bansal, and Christopher Ré. 2021. Robustness gym: Unifying the nlp evaluation landscape.
- Sepp Hochreiter, Jürgen Schmidhuber, et al. 1997. Long short-term memory. *Neural computation*, 9(8):1735–1780.
- Yoon Kim. 2014. Convolutional neural networks for sentence classification. In *Proceedings of the* 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP), pages 1746–1751, Doha, Qatar. Association for Computational Linguistics.
- Linyang Li, Ruotian Ma, Qipeng Guo, Xiangyang Xue, and Xipeng Qiu. 2020. Bert-attack: Adversarial attack against bert using bert. In *Proceedings of the* 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), pages 6193–6202.
- Xin Li, Lidong Bing, Wai Lam, and Bei Shi. 2018. Transformation networks for target-oriented sentiment classification. In *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 946–956.
- Dehong Ma, Sujian Li, Xiaodong Zhang, and Houfeng Wang. 2017. Interactive attention networks for aspect-level sentiment classification. In *Proceedings of the 26th International Joint Conference on Artificial Intelligence*, pages 4068–4074.
- Edward Ma. 2019. Nlp augmentation. https://github.com/makcedward/nlpaug.
- John Miller, Karl Krauth, Benjamin Recht, and Ludwig Schmidt. 2020. The effect of natural distribution shift on question answering models. In *International Conference on Machine Learning*, pages 6905–6916. PMLR.
- John X Morris, Eli Lifland, Jin Yong Yoo, and Yanjun Qi. 2020. Textattack: A framework for adversarial attacks in natural language processing. *arXiv preprint arXiv:2005.05909*.
- Harsha Nori, Samuel Jenkins, Paul Koch, and Rich Caruana. 2019. Interpretml: A unified framework for machine learning interpretability.
- Marco Tulio Ribeiro, Tongshuang Wu, Carlos Guestrin, and Sameer Singh. 2020. Beyond accuracy: Behavioral testing of NLP models with CheckList.

373.

In Proceedings of the 58th Annual Meeting of the

Association for Computational Linguistics, pages

4902–4912, Online. Association for Computational

Duyu Tang, Bing Qin, Xiaocheng Feng, and Ting

Liu. 2016a. Effective lstms for target-dependent

sentiment classification. In Proceedings of COLING

2016, the 26th International Conference on Compu-

tational Linguistics: Technical Papers, pages 3298-

Duyu Tang, Bing Qin, and Ting Liu. 2016b. Aspect

level sentiment classification with deep memory

network. In Proceedings of the 2016 Conference on

Empirical Methods in Natural Language Processing,

Erik F. Tjong Kim Sang and Fien De Meulder.

2003. Introduction to the CoNLL-2003 shared task:

Language-independent named entity recognition. In

Proceedings of the Seventh Conference on Natural Language Learning at HLT-NAACL 2003, pages

Eric Wallace, Jens Tuyls, Junlin Wang, Sanjay Subramanian, Matt Gardner, and Sameer Singh. 2019.

AllenNLP interpret: A framework for explaining

predictions of NLP models. 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): System Demonstrations, pages

7-12, Hong Kong, China. Association for Compu-

Yequan Wang, Minlie Huang, Xiaoyan Zhu, and

Tongshuang Wu, Marco Tulio Ribeiro, Jeffrey Heer,

Proceedings of the 57th Annual Meeting of the

Association for Computational Linguistics, pages

Xiaoyu Xing, Zhijing Jin, Di Jin, Bingning Wang,

burgers, soggy fries: Probing aspect robustness in aspect-based sentiment analysis. In Proceedings

of the 2020 Conference on Empirical Methods

in Natural Language Processing (EMNLP), pages

Biging Zeng, Heng Yang, Ruyang Xu, Wu Zhou,

Guoyang Zeng, Fanchao Qi, Qianrui Zhou, Tingji

Zhang, Bairu Hou, Yuan Zang, Zhiyuan Liu, and

Maosong Sun. 2020. Openattack: An open-source

and Xuli Han. 2019. Lcf: A local context focus

mechanism for aspect-based sentiment classification.

Oi Zhang, and Xuan-Jing Huang. 2020.

reproducible, and testable error analysis.

Errudite: Scalable,

In

Tasty

language processing, pages 606–615.

and Daniel S Weld. 2019.

Applied Sciences, 9(16):3389.

747-763.

3594-3605.

Li Zhao. 2016. Attention-based lstm for aspect-

level sentiment classification. In Proceedings of the 2016 conference on empirical methods in natural

Linguistics.

3307.

pages 214–224.

142–147.

tational Linguistics.

700 701 702

- 703
- 704
- 705 706
- 707
- 708
- 709 710
- 712 713
- 714
- 715
- 716
- 717
- 718 719
- 720
- 721 722
- 723 724
- 725
- 726
- 727 728
- 729
- 730
- 731 732
- 733 734 735

736

737

- 738 739
- 740
- 741 742

743 744

745

746

- 747
- 748

749

textual adversarial attack toolkit. arXiv preprint arXiv:2009.09191.

750

799

- 751 752 Jiawei Zhang, Yang Wang, Piero Molino, Lezhi Li, 753 and David S Ebert. 2018. Manifold: A modelagnostic framework for interpretation and diagnosis 754 of machine learning models. IEEE transactions 755 on visualization and computer graphics, 25(1):364-756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798
- 8