Enhancing Recurrent Neural Networks with Sememes

Yujia Qin\textsuperscript{1,*}, Fanchao Qi\textsuperscript{2,*}, Sicong Ouyang\textsuperscript{3†}, Zhiyuan Liu\textsuperscript{2}, Cheng Yang\textsuperscript{3}, Yasheng Wang\textsuperscript{4}, Qun Liu\textsuperscript{4}, Maosong Sun\textsuperscript{2}

\textsuperscript{1}Department of Electronic Engineering, Tsinghua University
\textsuperscript{2}Department of Computer Science and Technology, Tsinghua University
\textsuperscript{3}State Key Lab on Intelligent Technology and Systems, Tsinghua University
\textsuperscript{4}Beijing University of Posts and Telecommunications \textsuperscript{4}Huawei Noah’s Ark Lab

Abstract
Sememes, the minimum semantic units of human languages, have been successfully utilized in various natural language processing applications. However, most existing studies exploit sememes in specific tasks and few efforts are made to utilize sememes more fundamentally. In this paper, we propose to incorporate sememes into recurrent neural networks (RNNs) to improve their sequence modeling ability, which is beneficial to all kinds of downstream tasks. We design three different sememe incorporation methods and employ them in typical RNNs including LSTM, GRU and their bidirectional variants. For evaluation, we use several benchmark datasets involving PTB and WikiText-2 for language modeling, SNLI for natural language inference. Experimental results show evident and consistent improvement of our sememe-incorporated models compared with vanilla RNNs, which proves the effectiveness of our sememe incorporation methods. Moreover, we find that the sememe-incorporated models have great robustness and outperform adversarial training in defending adversarial attack. All the code and data of this work will be made available to the public.

Introduction
A word is the smallest unit of language, but its meaning can be split into smaller elements, i.e., sememes. In linguistics, a sememe is defined as the minimum unit of semantics (Bloomfield 1926). Some linguists have the opinion that the meanings of all the words can be represented with a limited set of sememes, which is similar to the idea of semantic primitives (Wierzbicka 1996). Considering sememes are usually implicit in words, researchers build sememe knowledge bases (KBs), which contain many words manually annotated with a set of predefined sememes, to utilize them. With the help of sememe KBs, sememes have been successfully applied to various natural language processing (NLP) tasks, e.g., word similarity computation (Liu and Li 2002), sentiment analysis (Fu et al. 2013), word representation learning (Niu et al. 2017) and lexicon expansion (Zeng et al. 2018). However, existing work usually exploits sememes for specific tasks and few efforts are made to utilize sememes in a more general and fundamental fashion. Gu et al. (2018) make an attempt to incorporate sememes into a long short-term memory (LSTM) (Hochreiter and Schmidhuber 1997) language model to improve its performance. Nevertheless, their method uses sememes in the decoder step only and as a result, it is not applicable to other sequence modeling tasks. To the best of our knowledge, no previous work tries to employ sememes to model better text sequences and achieve higher performance of downstream tasks.

In this paper, we propose to incorporate sememes into recurrent neural networks (RNNs) to improve their general sequence modeling ability, which is beneficial to all kinds of downstream NLP tasks. Some studies have tried to incorporate other linguistic knowledge into RNNs (Ahn et al. 2016; Yang and Mitchell 2017; Parthasarathi and Pineau 2018; Young et al. 2018). However, almost all of them utilize word-level KBs, which comprise relations between words, e.g., WordNet (Miller 1998) and ConceptNet (Speer and Havasi 2013). Different from these KBs, sememe KBs use semantically infra-word elements (sememes) to compositionally explain meanings of words and focus on the relations between sememes and words. Therefore, it is difficult to directly adopt previous methods to incorporate sememes into RNNs.

To tackle this challenge, we specifically design three methods of incorporating sememes into RNNs. All of them are highly adaptable and work on different RNN architecture. We employ these methods in two typical RNNs including LSTM, gated recurrent unit (GRU) and their bidirectional variants. In experiments, we evaluate the sememe-incorporated and vanilla RNNs on the benchmark datasets of two representative sequence modeling tasks, namely language modeling and natural language inference. Experimental results show that the sememe-incorporated RNNs achieve consistent performance improvement on all the tasks, which demonstrates the effectiveness of our sememe-incorporation methods and the usefulness of sememes. We also make a case study to explain the benefit of sememes in the task of natural language inference. Furthermore, we conduct an adversarial attack experiment, finding the sememe-incorporated RNNs display great robustness and perform much better than adversarial training.
In conclusion, our contribution consists in: (1) making the first exploration of utilizing sememes to improve the general sequence modeling ability of RNNs; and (2) proposing three effective and highly adaptable methods of incorporating sememes into RNNs.

Background

In this section, we first introduce the sememe annotation in HowNet, the sememe KB we utilize. Then we give a brief introduction to two typical RNNs, namely LSTM and GRU, together with their bidirectional variants.

Sememe Annotation in HowNet

HowNet [Dong and Dong 2003] is one of the most famous sememe KBs, which contains over 100 thousand Chinese and English words annotated with about 2,000 predefined sememes. Sememe annotation in HowNet is sense-level. In other words, each sense of polysemous words is annotated with one or more sememes with hierarchical structures. Figure 1 illustrates the sememe annotation of the word “cardinal” in HowNet. As shown in the figure, “cardinal” has two senses in HowNet, namely “cardinal (important)” and “cardinal (bishop)”. The former sense is annotated with only one sememe important, while the latter sense has one main sememe human and three subsidiary sememes including religion, official and ProperName.

In this paper, we focus on the meanings of sememes and ignore their hierarchical structures for simplicity. Thus, we simply equip each word with a sememe set, which comprises all the sememes annotated to the senses of the word. For instance, the sememe set of “cardinal” is \{important, human, religion, official, ProperName\}. We leave the utilization of sememe structures for future work.

Introduction to Typical RNNs

RNN is a class of artificial neural network designed for processing temporal sequences. LSTM and GRU are two of the most predominant RNNs. They have been widely used in recent years owing to their superior sequence modeling ability.

An LSTM consists of multiple identical cells and each cell corresponds to a token in the input sequence. For each cell, it takes the embedding of the corresponding token \(x_t\) as input to update its cell state \(c_t\) and hidden state \(h_t\). Different from the basic RNN, LSTM integrates a forget gate \(f_t\), an input gate \(i_t\) and an output gate \(o_t\) into its cell, which can alleviate the gradient vanishing issue of the basic RNN. Given the hidden state \(h_{t-1}\) and the cell state \(c_{t-1}\) of the previous cell, the cell state \(c_t\) and the hidden state \(h_t\) of the current cell can be computed by:

\[
\begin{align*}
    f_t &= \sigma(W_f [x_t; h_{t-1}] + b_f) \\
    i_t &= \sigma(W_i [x_t; h_{t-1}] + b_i) \\
    c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \\
    o_t &= \sigma(W_o [x_t; h_{t-1}] + b_o) \\
    h_t &= o_t \odot \tanh(c_t)
\end{align*}
\]  

where \(W_f\), \(W_i\), \(W_o\) and \(W_o\) are weight matrices, and \(b_f\), \(b_i\), \(b_c\) and \(b_o\) are bias vectors. \(\sigma\) is the sigmoid function, \([\ ]\) denotes the concatenation operation and \(*\) indicates element-wise multiplication. The structure of an LSTM cell is illustrated in the upper left corner of Figure 2.

GRU is another popular extension of the basic RNN. It has fewer gates than LSTM. In addition to the input \(x_t\) and hidden state \(h_t\), each GRU cell embodies a update gate \(z_t\) and a reset gate \(r_t\). The transition equations of GRU are as follows:

\[
\begin{align*}
    z_t &= \sigma(W_z [x_t; h_{t-1}] + b_z) \\
    r_t &= \sigma(W_r [x_t; h_{t-1}] + b_r) \\
    \tilde{h}_t &= \tanh(W_h [x_t; r_t \odot h_{t-1}] + b_h) \\
    h_t &= (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t
\end{align*}
\]  

where \(W_z\), \(W_r\), \(W_h\) are weight matrices, and \(b_z\), \(b_r\), \(b_h\) are bias vectors. The lower left corner of Figure 2 shows the structure of a GRU cell.

Since both LSTM and GRU can only process sequences unidirectionally, their bidirectional variants, namely BiLSTM and BiGRU, are proposed to eliminate the restriction. BiLSTM and BiGRU have two sequences of cells: one processes the input sequence from left to right and the other from right to left. Hence, each token in the input sequence corresponds two unidirectional hidden states, which are concatenated into bidirectional hidden states:

\[
[\begin{array}{c}
\overrightarrow{h_1}, \overrightarrow{h_2}, ..., \overrightarrow{h_T} \\
\overleftarrow{h_1}, \overleftarrow{h_2}, ..., \overleftarrow{h_T}
\end{array}] = \begin{bmatrix}
\overrightarrow{h_1}, \overrightarrow{h_2}, ..., \overrightarrow{h_T} \\
\overleftarrow{h_1}, \overleftarrow{h_2}, ..., \overleftarrow{h_T}
\end{bmatrix},
\]

where \(T\) denotes the length of the input sequence.

Sememe Incorporation Methods

In this section, we elaborately describe three methods of incorporating sememes into RNNs, namely simple concatenation (+concat), adding sememe output gate (+gate) and introducing sememe-RNN cell (+cell). All the three methods are applicable to both LSTM and GRU, both unidirectional and bidirectional RNNs. The following descriptions are based on unidirectional LSTM and GRU, and the newly added variables and formulae are underlined for clarity. Bidirectional sememe-incorporated LSTMs and GRUs are just a trivial matter of concatenating the hidden states of
can directly add the bedding to the cardinality of a set. We concatenate its original word embedding via its input (word embedding). Formally, given a word $x_t$, its sememe set is $S_t = \{s_1, \cdots, s_{|S_t|}\}$, where $|·|$ denotes the cardinality of a set. We concatenate its original word embedding $x_t$ with sememe embedding $\pi_t$:

$$\pi_t = \sum_{s \in S_t} s \tilde{x}_t = [x_t; \pi_t] \quad (4)$$

where $s$ denotes the sememe embedding of $s$, and $\tilde{x}_t$ is the retrofitted word embedding which incorporates sememe knowledge.

Adding Sememe Output Gate

In the first method, sememe knowledge is shallowly incorporated into RNN cells. It is essentially a kind of enhancement of word embeddings. Inspired by Ma, Peng, and Cambria (2018), we propose the second method which enables deep incorporation of sememes into RNN cells. More specifically, we add an additional sememe output gate $o_t^s$ to the vanilla RNN cell, which decides how much sememe knowledge is absorbed into the hidden state. Meanwhile, the original gates are also affected by the sememe knowledge term. The transition equations of LSTM with the sememe output gate are as follows:

$$f_t = \sigma(W_f[x_t; h_{t-1}; \pi_t] + b_f)$$
$$i_t = \sigma(W_i[x_t; h_{t-1}; \pi_t] + b_i)$$
$$\tilde{c}_t = \tanh(W_c[x_t; h_{t-1}] + b_c)$$
$$c_t = f_t \cdot c_{t-1} + i_t \cdot \tilde{c}_t$$
$$o_t = \sigma(W_o[x_t; h_{t-1}; \pi_t] + b_o)$$
$$o_t^s = \sigma(W_o^s[x_t; h_{t-1}; \pi_t] + b_{o^s})$$
$$h_t = o_t \cdot \tanh(c_t) + o_t^s \cdot \tanh(W_c \pi_t) \quad (5)$$

where $W_o$ is a weight matrix and $b_o$ is a bias vector.

We can find that $o_t^s \cdot \tanh(W_c \pi_t)$ can directly add the term of sememe knowledge to the original hidden state. By doing this, the original hidden state, which carries contextual information only, is enhanced by semantic information of sememe knowledge.

The sememe output gate can be added to GRU in a similar way, and the transition equations are as follows:

$$z_t = \sigma(W_z[x_t; h_{t-1}; \pi_t] + b_z)$$
$$r_t = \sigma(W_r[x_t; h_{t-1}; \pi_t] + b_r)$$
$$\tilde{h}_t = \sigma(W_o[x_t; h_{t-1}; \pi_t] + b_o)$$
$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tilde{h}_t + o_t^s \cdot \tanh(\pi_t) \quad (6)$$

where $o_t^s$ is the sememe output gate, $W_o$ is a weight matrix and $b_o$ is a bias vector.

Introducing Sememe-RNN Cell

In the second method, although sememe knowledge is incorporated into RNN cells directly and deeply, it can be utilized
more sufficiently. Taking LSTM for example, as shown in Equation (5), the hidden state $h_t$ comprises two parts. The first part is the contextual information item $c_t \ast \tanh(c_t)$. It bears the information of current word and preceding text, which has been processed by the forget gate and encoded into the cell state. The second part is the sememe knowledge item $o_t \ast \tanh(W_o \pi_t)$. It carries the information of sememe knowledge which has not processed or encoded. Therefore, the two parts are inconsistent.

To address the issue, we propose the third sememe incorporation method. We regard the sememe knowledge as another information source like the previous word and introduce an extra RNN cell to encode it. Specifically, we first feed the sememe knowledge embedding to an LSTM cell (sememe-LSTM cell) and obtain its cell and hidden states which carry sememe knowledge. Then we design a special forget gate for the sememe knowledge and use it to process the cell state of the sememe-LSTM cell, just as the previous cell state. Finally, we add the processed cell state of the sememe-LSTM to the original cell state. In addition, the hidden state of the sememe-LSTM cell is also absorbed into the input gate and output gate. Formally, the transition equations of LSTM with the sememe-LSTM cell are as follows:

$$
\begin{align*}
    c^*_t, \ h^*_t &= \text{LSTM}^{(S)}(\pi_t) \\
    f_t &= \sigma(W_f [x_t; h_{t-1}] + b_f) \\
    f^*_t &= \sigma(W_f^* [x_t; h^*_t] + b_f^*) \\
    i_t &= \sigma(W_{i} [x_t; h_{t-1}; h^*_t] + b_i) \\
    c_t &= f_t \ast c_{t-1} + f^*_t \ast c^*_t + i_t \ast \tilde{c}_t \\
    h_t &= o_t \ast \tanh(c_t)
\end{align*}
$$

where $c^*_t$ and $h^*_t$ are the cell state and hidden state of the sememe-LSTM cell, $f^*_t$ is the sememe forget gate, $W_f^*$ is a weight matrix and $b_f^*$ is a bias vector.

Similarly, we can introduce a sememe-GRU cell to the original GRU and the transition equations are as follows:

$$
\begin{align*}
    h^*_t &= \text{GRU}^{(S)}(\pi_t) \\
    z_t &= \sigma(W_z [x_t; h_{t-1}; h^*_t] + b_z) \\
    r_t &= \sigma(W_r [x_t; h_{t-1}; h^*_t] + b_r) \\
    \tilde{h}_t &= \tanh(W_h [x_t; r_t \ast (h_{t-1} + h^*_t)] + b_h) \\
    h_t &= (1 - z_t) \ast h_{t-1} + z_t \ast \tilde{h}_t
\end{align*}
$$

where $h^*_t$ is the hidden state of the sememe-GRU cell.

Language Modeling

In this section, we evaluate our sememe-incorporate RNNs on the task of language modeling (LM).

Dataset

We use two benchmark LM datasets, namely Penn Treebank (PTB) (Marcus, Santorini, and Marcinkiewicz 1993) and WikiText-2 (Merity et al. 2016). PTB is made up of articles from the Wall Street Journal. Its vocabulary size is 10,000. The token numbers of its training, validation and test sets are 887, 521, 70, 390 and 78, 669 respectively. WikiText-2 comprises Wikipedia articles and its vocabulary size is 33, 278. It has 2, 088, 628, 217, 646 and 245, 569 tokens in its training, validation and test sets.

We choose HowNet as the source of sememes. It contains 2, 186 different sememes and 43, 321 English words with sememe annotation. The numbers of sememe-annotated tokens in PTB and WikiText-2 are 870, 520 (83.98%) and 2, 068, 779 (81.07%) respectively.

Experimental Settings

Baseline Methods We choose the vanilla LSTM and GRU as the baseline methods. Notice that bidirectional RNNs are generally not used in the LM task because they are not allowed to know the whole sentence.

Hyper-parameters Following previous work, we try the models on two sets of hyper-parameters, namely “medium” and “large”. For “medium”, the dimension of hidden states and word/sememe embeddings is set to 650, the batch size is 20, and the dropout rate is 0.5. For “large”, the dimension of vectors is 1500, the dropout rate is 0.65, and other hyper-parameters are the same as “medium”. All the word and sememe embeddings are randomly initialized as real-valued vectors using a normal distribution with mean 0 and variance 0.05. The above-mentioned hyper-parameter settings are applied to all the models.

Training Strategy We also adopt the same training strategy for all the models. We choose stochastic gradient descent (SGD) as the optimizer, whose initial learning rate is 20 for LSTM and 10 for GRU. The learning rate would be divided by 4 if no improvement is observed on the validation set. The maximum training epoch number is 40 and the gradient norm clip boundary is 0.25.

Experimental Results

Table 1 shows the perplexity results on both validation and test sets of the two datasets. From the table, we can observe that:

1. All the sememe-incorporated RNNs, including the simplest “+concat” models, achieve lower perplexity as compared to corresponding vanilla RNNs, which demonstrates the usefulness of sememes for enhancing sequence modeling and the effectiveness of our sememe incorporation methods;

2. Among the three different methods, “+cell” performs best for LSTM and “+gate” performs best for GRU at both “medium” and “large” hyper-parameter settings. The possible explanation is that “+cell” incorporates limited sememe knowledge into GRU as compared to LSTM. In fact, GRU+cell is much less affected by sememe knowledge than GRU+gate, as shown in Equation (8).
### Table 1: Perplexity results of all the models on the validation and test sets of PTB and WikiText-2.

| Dataset   | PTB Validation | PTB Test | WikiText-2 Validation | WikiText-2 Test |
|-----------|----------------|----------|-----------------------|------------------|
| LSTM(medium) | 85.14         | 81.74    | 98.87                 | 93.69            |
| +concat    | 81.79         | 78.90    | 96.05                 | 91.41            |
| +gate      | 81.15         | 77.73    | 95.27                 | 90.19            |
| +cell      | **79.71**     | **76.57**| **94.49**             | **89.39**        |
| LSTM(large) | 81.88         | 78.34    | 96.86                 | 91.07            |
| +concat    | 78.35         | 75.25    | 92.72                 | 87.51            |
| +gate      | 77.02         | 73.90    | 91.02                 | 86.16            |
| +cell      | **76.47**     | **73.01**| **90.44**             | **85.62**        |
| GRU(medium) | 94.84         | 91.05    | 109.11                | 103.07           |
| +concat    | 90.68         | 87.29    | 105.11                | 98.89            |
| +gate      | **88.87**     | **85.12**| **103.13**            | **96.97**        |
| +cell      | 89.56         | 86.49    | 103.53                | 97.65            |
| GRU(large)  | 92.68         | 89.60    | 107.75                | 101.52           |
| +concat    | 91.64         | 87.62    | 104.33                | 98.15            |
| +gate      | **88.08**     | **84.49**| **102.84**            | **96.71**        |
| +cell      | 89.33         | 86.05    | **101.22**            | **95.67**        |

(3) By comparing the results of the “large” vanilla RNNs and the “medium” sememe-incorporated RNNs, we can exclude the possibility that better performance of the sememe-incorporated RNNs is brought by more parameters. For example, the perplexity of the “large” vanilla LSTM and the “medium” LSTM+cell on the four sets is 81.88/79.71, 78.34/76.57, 96.86/94.49 and 91.07/89.39 respectively. Although the “large” vanilla LSTM has much more parameters than “medium” LSTM+cell (76M vs. 24M), it is still outperformed by the latter.

### Natural Language Inference

Natural language inference (NLI), also known as recognizing textual entailment, is a classic sentence pair classification task. In this section, we evaluate our models on the NLI task.

#### Dataset

We choose the most famous benchmark dataset, Stanford Natural Language Inference (SNLI) (Bowman et al. 2015) dataset for evaluation. It contains 570k sentence pairs, each of which comprises a premise and a hypothesis. The relations of the sentence pairs are manually classified into 3 categories, namely “entailment”, “contradiction” and “neutral”. In addition, the coverage of its sememe-annotated tokens is 82.31%.

#### Experimental Settings

**Baseline Methods** In addition to vanilla LSTM, GRU and their bidirectional variants, we design two extra baseline methods. For the first one, we randomly assign each word some meaningless labels in the same quantity as its sememes and substitute sememes by these labels, where the total number of different labels is also equal to that of sememes. For the second one, we use WordNet as the source of external knowledge and substitute the sememes of a word by its synonyms with same POS tag.

#### Hyper-parameters

We use 300-dimensional word embeddings pre-trained by GloVe (Pennington, Socher, and Manning 2014), which are frozen during training. Embeddings of sememes and meaningless labels are randomly initialized as 300-dimensional real-valued vectors using a normal distribution with mean 0 and variance 0.05. The dropout rate for input word embedding is 0.2. The dimension of hidden states is 2048. In addition, other hyper-parameters are the same as those of the LM experiment.

#### Training Strategy

We still choose the SGD optimizer, whose initial learning rate is 0.1 and weight factor is 0.99. We divide the learning rate by 5 if no improvement is observed on the validation dataset.

#### Classifier

Following previous work (Bowman et al. 2016; Mou et al. 2016), we employ a three-layer perceptron plus a three-way softmax layer as the classifier, whose input is a feature vector constructed from the embeddings of a pair of sentences. Specifically, we use any RNN model to process the two sentences of a premise-hypothesis pair and obtain their embeddings $h_{pre}$ and $h_{hyp}$. Then we construct the feature vector $v$ as follows:

$$ v = \begin{bmatrix} h_{pre} \\ h_{hyp} \\ |h_{pre} - h_{hyp}| \\ h_{pre} \ast h_{hyp} \end{bmatrix}. \tag{9} $$

#### Experimental Results

Table 2 lists the results of all the models on the test set of SNLI. From this table, we can see that:

(1) All the sememe-incorporated models achieve marked performance enhancement compared with corresponding vanilla models, which proves the usefulness of sememes in improving the sentence representation ability of RNNs and the effectiveness of our sememe incorporation methods;
Entailment Example
Premise: Four men stand in a circle facing each other playing [perform, reaction, MusicTool] brass instruments [MusicTool, implement] which people watch them.
Hypothesis: The men are playing music [music].

Contradict Example
Premise: A group of women playing volleyball indoors [location, house, internal].
Hypothesis: People are outside [location, external] tossing a ball.

Table 3: Two examples of premise-hypothesis pairs in the SNLI dataset. The words in italic type are important words and their sememes are appended.

(2) By comparing the results of the models with the same knowledge incorporation method but different external knowledge, the superiority of sememes is further confirmed. When sememes are substituted by meaningless labels or WordNet synonyms, the performance of any knowledge-incorporated model declines and becomes even worse than that of vanilla RNNs.

(3) Among the three sememe incorporation methods, “+cell” achieves the best overall performance, which manifests the great efficiency of “+cell” in utilizing sememe knowledge. This is also consistent with the conclusion of the LM experiment basically.

Case Study
In this subsection, we use two examples to illustrate how sememes are beneficial to handling the task of NLI. Table 3 exhibits two premise-hypothesis pairs in the SNLI dataset, where the sememes of some important words are appended to corresponding words.

For the first premise-hypothesis pair, its relation type is annotated as “entailment” in SNLI. Our sememe-incorporated models yield the correct result while all the baseline methods do not. We notice that there are several important words whose sememes provide useful information. In the premise, both the words “playing” and “instruments” have the sememe MusicTool, which is semantically related to the sememe music of the word “music” in the hypothesis. We speculate that the semantic relatedness given by sememes assists our models in coping with this sentence pair.

The second premise-hypothesis pair, whose true relation is “contradict”, is also classified correctly by our models but wrongly by the baseline methods. We find that the word “indoors” in the premise has the sememe internal, while the word “outside” in the hypothesis has the sememe external. The two sememes are a pair of antonyms, which may explain why our models make the right judgment.

Adversarial Attack Experiment
Adversarial attack and defense have attracted considerable research attention recently (Szegedy et al. 2014, Goodfellow et al., 2015), because they can disclose and fix the vulnerability of neural networks that small perturbations of input can cause significant changes of output. Adversarial attack is aimed at generating adversarial examples to fool a neural model (victim model) and adversarial defense is targeted at improving the robustness of the model against attack. In the field of NLP, all kinds of adversarial attack methods have been proposed (Zhang, Sheng, and Alhazmi 2019) but few efforts are made in adversarial defense (Wang et al. 2019).

We intuitively believe that incorporating sememes can improve the robustness of neural networks, because sememes are general linguistic knowledge and complementary to text corpora on which neural networks heavily rely. Therefore, we evaluate the robustness of our sememe-incorporated RNNs against adversarial attack.

Attack Method
We use a genetic algorithm-based attack model (Alzantot et al. 2018), which is a typical gradient-free black-box attack method. It generates adversarial examples by substituting words of model input iteratively and achieves impressive attack performance on both sentiment analysis and NLI.

Baseline Methods
Besides the WordNet-incorporated RNNs, we choose adversarial training (Madry et al. 2015) as the baseline methods. Adversarial training is believed to be an effective defense method. It adds some generated adversarial examples to the training set, aiming to generalize the victim model to the adversarial attack.

Experimental Settings
For the attack method, we use all the recommended hyper-parameters of its original work (Alzantot et al. 2018). For the victim models including vanilla RNNs together with their sememe and WordNet-incorporated versions, the hyper-parameters and training strategy are the same as those in the previous experiment. For adversarial training, we add 57k (10% of the number of total sentence pairs in SNLI) generated adversarial examples (premise-hypothesis pairs) to the training set. We use the attack success rate (%) as the evaluation metric. The lower the attack success rate is, the more robust a model is.

Experimental Results
Table 4 lists the success rates of adversarial attack against all the victim models. We can observe that:

(1) The attack success rates of our sememe-incorporated RNNs are consistently lower than those of the vanilla RNNs, which indicates the sememe-incorporated RNNs have greater robustness against adversarial attack. Furthermore, the experimental results also verify the effectiveness of sememes in improving robustness of neural networks.

(2) Among the three sememe incorporation methods, “+cell” beats the other two once again. It demonstrates the advantage of “+cell” in properly incorporating sememes into RNNs.
In this paper, we make the first attempt to incorporate sememes into RNNs to enhance their sequence modeling ability, which is beneficial to many downstream NLP tasks. We preliminarily propose three highly adaptable sememe incorporation methods, and employ them in typical RNNs including LSTM, GRU and their bidirectional versions. In experiments, we evaluate our methods on the benchmark datasets of language modeling and natural language inference. Experimental results show that sememe-incorporated RNNs achieve obvious performance improvement, which demonstrates the usefulness of sememes and effectiveness of our methods.

In the future, we will explore following directions including: (1) considering the hierarchical structures of sememes, which contain more semantic information of words; (2) using attention mechanism to adjust the weights of sememes in different context to take better advantage of sememes; (3) evaluating our sememe-incorporated RNNs on other sequence modeling tasks; and (4) incorporating sememe knowledge into other neural models such as the transformer.

### Conclusion and Future Work

| Knowledge | Model | LSTM | GRU | BiLSTM | BiGRU |
|-----------|-------|------|-----|--------|-------|
| None      | vanilla | 64.8 | 65.4 | 63.9 | 64.7 |
| None      | vanilla+at | 66.2 | 67.4 | 65.9 | 66.3 |
| WordNet   | +concat | 63.2 | 66.4 | 63.6 | 64.8 |
|           | +gate   | 64.7 | 65.6 | 63.8 | 64.2 |
|           | +cell   | 64.3 | 66.1 | 64.5 | 63.9 |
| Sememe    | +concat | 64.5 | 65.3 | 63.3 | 64.2 |
|           | +gate   | 62.9 | 65.1 | 62.5 | 63.6 |
|           | +cell   | 63.9 | 64.9 | 62.3 | 63.2 |

Table 4: Success rates (%) of adversarial attack against all the defense models on the test set of SNLI. “vanilla+at” represents adversarial training.

(3) Some models incorporated with WordNet have lower attack success rates than corresponding vanilla RNNs. However, from an overall perspective, incorporating WordNet into RNNs only brings negligible decrease of the attack access rate. It indicates WordNet has very limited capability to improve the robustness of neural networks, especially compared with sememes.

(4) Adversarial training increases the attack success rates of all the models rather than decrease them, which is consistent with the findings of previous work [Alzantot et al. 2018]. It shows adversarial training is not an effective defense method, at least for the attack we use. In fact, there are few effective adversarial defense methods, which makes the superiority of sememes in defending adversarial attack and improving robustness of models more valuable.

### Related Work

#### HowNet and Its Applications

HowNet [Dong and Dong 2003] is one of the most famous sememe KBs, whose construction takes several linguistic experts more than two decades. After HowNet is published, it has been employed in diverse NLP tasks including word similarity computation [Liu and Li 2002], word representation learning [Niu et al. 2017], word sense disambiguation [Duan, Zhao, and Xu 2007], sentiment analysis [Dang and Zhang 2010], lexicon expansion [Zeng et al. 2018], etc. There are also some studies trying to expand HowNet [Xie et al. 2017], [Jin et al. 2018] and transfer its sememe knowledge to other languages [Qi et al. 2018].

Gu et al. [2018] exploit sememes in a sequence modeling task (language modeling) for the first time. They add a sememe predictor to an LSTM language model, which is aimed at predicting sememes of the next word using preceding text. Then they use the predicted sememes to predict the next word. Nevertheless, their method uses sememes in the decoder step of the LSTM language model and does not improve the LSTM's ability to encode sequences. Therefore, it cannot be applied to other sequence modeling tasks. As far as we know, we are the first to utilize sememes to improve general sequence modeling ability of neural networks.

### Recurrent Neural Networks

The recurrent neural network (RNN) [Rumelhart et al. 1988] and its representative extensions including LSTM [Hochreiter and Schmidhuber 1997] and GRU [Cho et al. 2014], have been widely employed in various NLP tasks, e.g., language modeling [Mikolov et al. 2010], sentiment analysis [Nakov et al. 2016], semantic role labeling [He et al. 2018], dependency parsing [Kiperwasser and Goldberg 2016] and natural language inference [Parikh et al. 2016].

To improve the sequence modeling ability of RNNs, some researches try to reform the frameworks of RNNs, e.g., integrating the attention mechanism [Bachman and Precup 2015], adding hierarchical structures [Schmidhuber 1992] and introducing bidirectional modeling [Graves, Fernández, and Schmidhuber 2005].

In addition, some work focuses on incorporating different kinds of external knowledge into RNNs. General linguistic knowledge from famous KBs such as WordNet [Miller 1998] and ConceptNet [Speer and Havasi 2013] attracts considerable attention. These KBs usually comprise relations between words, which are hard to be incorporated into the internal structures of RNNs. Therefore, most existing knowledge-incorporated methods employ external linguistic knowledge on the hidden layers of RNNs rather than the internal structures of RNN cells. (Ahn et al. 2016, Yang and Mitchell 2017, Parthasarathi and Pineau 2018, Young et al. 2018).

Since sememe knowledge is very different from the word-level relational knowledge, it cannot be incorporated into RNNs with the same methods. As far as we know, no previous work tries to incorporate such knowledge as sememes into RNNs.
References

[Ahn et al. 2016] Ahn, S.; Choi, H.; Pärnamaa, T.; and Bengio, Y. 2016. A neural knowledge language model. arXiv preprint arXiv:1608.00318.

[Alzantot et al. 2018] Alzantot, M.; Sharma, Y.; Elgohary, A.; Ho, B.-J.; Srivastava, M.; and Chang, K.-W. 2018. Generating natural language adversarial examples. In Proceedings of EMNLP.

[Bachman and Precup 2015] Bachman, P., and Precup, D. 2015. Variational generative stochastic networks with collaborative shaping. In Proceedings of ICML.

[Bloomfield 1926] Bloomfield, L. 1926. A set of postulates for the science of language. Language 2(3):153–164.

[Bowman et al. 2015] Bowman, S. R.; Angeli, G.; Potts, C.; and Manning, C. D. 2015. A large annotated corpus for learning natural language inference. In Proceedings of EMNLP.

[Bowman et al. 2016] Bowman, S. R.; Gauthier, J.; Rastogi, A.; Gupta, R.; Manning, C. D.; and Potts, C. 2016. A fast unified model for parsing and sentence understanding. In Proceedings of ACL.

[Cho et al. 2014] Cho, K.; Van Merriéenboer, B.; Gulcehre, C.; Bahdanau, D.; Bougares, F.; Schwenk, H.; and Bengio, Y. 2014. Learning phrase representations using rnn encoder-decoder for statistical machine translation. In Proceedings of EMNLP.

[Dang and Zhang 2010] Dang, L., and Zhang, L. 2010. Method of discriminant for chinese sentence sentiment orientation based on hownet. Application Research of Computers 4:43.

[Dong and Dong 2003] Dong, Z., and Dong, Q. 2003. Hownet-a hybrid language and knowledge resource. In Proceedings of NLPKE.

[Duan, Zhao, and Xu 2007] Duan, X.; Zhao, J.; and Xu, B. 2007. Word sense disambiguation through sememe labeling. In Proceedings of IJCAI.

[Du et al. 2013] Du, X.; Li, L.; and Li, Y. 2013. Multi-aspect sentiment analysis for chinese online social reviews based on topic modeling and hownet lexicon. Knowledge-Based Systems 37:186–195.

[Goodfellow, Shlens, and Szegedy 2015] Goodfellow, I. J.; Shlens, J.; and Szegedy, C. 2015. Explaining and harnessing adversarial examples. In Proceedings of ICLR.

[Graves, Fernández, and Schmidhuber 2005] Graves, A.; Fernández, S.; and Schmidhuber, J. 2005. Bidirectional lstm networks for improved phoneme classification and recognition. In Proceedings of International Conference on Artificial Neural Networks.

[Gu et al. 2018] Gu, Y.; Yan, J.; Zhu, H.; Liu, Z.; Xie, R.; Sun, M.; Lin, F.; and Lin, L. 2018. Language modeling with sparse product of sememe experts. In Proceedings of EMNLP.

[He et al. 2018] He, L.; Lee, K.; Levy, O.; and Zettlemoyer, L. 2018. Jointly predicting predicates and arguments in neural semantic role labeling. In Proceedings of ACL.

[Hochreiter and Schmidhuber 1997] Hochreiter, S., and Schmidhuber, J. 1997. Long short-term memory. Neural Computation 9(8):1735–1780.

[Jin et al. 2018] Jin, H.; Zhu, H.; Liu, Z.; Xie, R.; Sun, M.; Lin, F.; and Lin, L. 2018. Incorporating chinese characters of words for lexical sememe prediction. In Proceedings of ACL.

[Kiperwasser and Goldberg 2016] Kiperwasser, E., and Goldberg, Y. 2016. Simple and accurate dependency parsing using bidirectional lstm feature representations. TACL 4:313–327.

[Liu and Li 2002] Liu, Q., and Li, S. 2002. Word similarity computing based on hownet. International Journal of Computational Linguistics & Chinese Language Processing 7(2):59–76.

[Ma, Peng, and Cambria 2018] Ma, Y.; Peng, H.; and Cambria, E. 2018. Targeted aspect-based sentiment analysis via embedding commonsense knowledge into an attentive lstm. In Proceedings of AAAI.

[Mady et al. 2015] Mady, A.; Makelov, A.; Schmidt, L.; Tsipras, D.; and Vladu, A. 2015. Towards deep learning models resistant to adversarial attacks. In Proceedings of ICLR.

[Marcus, Santorini, and Marcinkiewicz 1993] Marcus, M.; Santorini, B.; and Marcinkiewicz, M. A. 1993. Building a large annotated corpus of english: The penn treebank. Computational Linguistics 19(2).

[Merity et al. 2016] Merity, S.; Xiong, C.; Bradbury, J.; and Socher, R. 2016. Pointer sentinel mixture models. arXiv preprint arXiv:1609.07843.

[Mikolov et al. 2010] Mikolov, T.; Karafiát, M.; Burget, L.; Černocký, J.; and Khudanpur, S. 2010. Recurrent neural network based language model. In Proceedings of Eleventh Annual Conference of the International Speech Communication Association.

[Miller 1998] Miller, G. 1998. WordNet: An electronic lexical database. MIT press.

[Mou et al. 2016] Mou, L.; Men, R.; Li, G.; Xu, Y.; Zhang, L.; Yan, R.; and Jin, Z. 2016. Natural language inference by tree-based convolution and heuristic matching. In Proceedings of ACL.

[Nakov et al. 2016] Nakov, P.; Ritter, A.; Rosenthal, S.; Sebastiani, F.; and Stoyanov, V. 2016. SemEval-2016 task 4: Sentiment analysis in twitter. In Proceedings of SemEval.

[Niu et al. 2017] Niu, Y.; Xie, R.; Liu, Z.; and Sun, M. 2017. Improved word representation learning with sememes. In Proceedings of ACL.

[Parikh et al. 2016] Parikh, A. P.; Täckström, O.; Das, D.; and Uszkoreit, J. 2016. A decomposable attention model for natural language inference. In Proceedings of EMNLP.

[Parthasarathi and Pineau 2018] Parthasarathi, P., and Pineau, J. 2018. Extending neural generative conversational model using external knowledge sources. In Proceedings of EMNLP.

[Pennington, Socher, and Manning 2014] Pennington, J.; Socher, R.; and Manning, C. D. 2014. Glove: Global vectors for word representation. In Proceedings of EMNLP.

[Qi et al. 2018] Qi, F.; Lin, Y.; Sun, M.; Zhu, H.; Xie, R.; and Liu, Z. 2018. Cross-lingual lexical sememe prediction. In Proceedings of EMNLP.

[Rumelhart et al. 1988] Rumelhart, D. E.; Hinton, G. E.; Williams, R. J.; et al. 1988. Learning representations by back-propagating errors. Cognitive modeling 5(3):1.

[Schmidhuber 1992] Schmidhuber, J. 1992. Learning complex, extended sequences using the principle of history compression. Neural Computation 4(2):234–242.

[Speer and Havasi 2013] Speer, R., and Havasi, C. 2013. ConceptNet 5: A large semantic network for relational knowledge. In The Peoples Web Meets NLP. Springer. 161–176.

[Szegedy et al. 2014] Szegedy, C.; Zaremba, W.; Sutskever, I.; Bruna, J.; Erhan, D.; Goodfellow, I.; and Fergus, R. 2014. Intriguing properties of neural networks. In Proceedings of ICLR.

[Wang et al. 2019] Wang, W.; Tang, B.; Wang, R.; Wang, L.; and Ye, A. 2019. A survey on adversarial attacks and defenses in text. arXiv preprint arXiv:1902.07285.
[Wierzbicka 1996] Wierzbicka, A. 1996. *Semantics: Primes and universals: Primes and universals*. Oxford University Press, UK.

[Xie et al. 2017] Xie, R.; Yuan, X.; Liu, Z.; and Sun, M. 2017. Lexical sememe prediction via word embeddings and matrix factorization. In Proceedings of AAAI.

[Yang and Mitchell 2017] Yang, B., and Mitchell, T. 2017. Leveraging knowledge bases in lstms for improving machine reading. In Proceedings of ACL.

[Young et al. 2018] Young, T.; Cambria, E.; Chaturvedi, I.; Zhou, H.; Biswas, S.; and Huang, M. 2018. Augmenting end-to-end dialogue systems with commonsense knowledge. In Proceedings of AAAI.

[Zeng et al. 2018] Zeng, X.; Yang, C.; Tu, C.; Liu, Z.; and Sun, M. 2018. Chinese liwc lexicon expansion via hierarchical classification of word embeddings with sememe attention. In Proceedings of AAAI.

[Zhang, Sheng, and Alhazmi 2019] Zhang, W. E.; Sheng, Q. Z.; and Alhazmi, A. A. F. 2019. Generating textual adversarial examples for deep learning models: A survey. arXiv preprint arXiv:1901.06796.