

# 基于深度学习的个性化聊天机器人研究

王乾铭, 李 吟

(江苏自动化研究所, 江苏 连云港 222006)

**摘要:** 为了对传统的聊天机器人局限性进行改进, 增强其回复时的个性化和多样化, 并使其具有一定的准确性, 研究改进了一种基于深度学习 Seq2Seq 模型的对话系统。对传统的编码器-解码器 (Encoder-Decoder) 模型进行了研究, 在原有模型的基础上使用了深度 LSTM 结构并且加入注意力机制使其能更好地适应不同长度的问句。在解码过程中, 将原有模型的贪心算法改为了 Beam Search 算法。在训练过程中, 利用了多次训练的方法, 训练出模拟电视剧角色的聊天机器人, 为聊天机器人赋予一个特定的身份。通过使用两种自动评估指标 BLEUs 和 Distinct-n 去测试聊天机器人, 并使用一些问句测试聊天机器人的反应, 最终实验结果表明新模型与原有的模型相比, 两种指标都取得了较好的效果, 并且输出句子的合理性以及回复质量也有明显的提高。

**关键词:** 聊天机器人; Seq2Seq 模型; 注意力机制; 多样性; 个性化

**中图分类号:** TP391

**文献标识码:** A

**文章编号:** 1673-629X(2020)04-0079-06

doi:10.3969/j.issn.1673-629X.2020.04.015

## Research on Personalized Chatbot Based on Deep Learning

WANG Qian-ming, LI Yin

(Jiangsu Automation Research Institute of CSIC, Lianyungang 222006, China)

**Abstract:** In order to improve the limitations of traditional chatbots, enhance the personalization and diversity of their replies, and make them accurate, a conversation system based on deep learning Seq2Seq model is improved. The traditional Encoder-Decoder model is studied, and the depth LSTM structure is used on the basis of the original model and the attention mechanism is added to make it better adapt to the questions of different lengths. In the decoding process, the greedy algorithm of the original model is changed to the Beam Search algorithm. In the training process, multiple training method is used to train the characters in TV series and give chatbot a specific identity. Two automatic evaluation indexes, BLEUs and Distinct-n, are used to test the chatbot whose response is tested by some questions. The final experiment shows that compared with the original model, the new model has achieved better results and improved the recovery quality.

**Key words:** chatbot; Seq2Seq model; attention mechanism; diversity; personality

## 0 引言

在学术界, 深度学习被广泛应用于各种研究领域, 在工业界, 深度学习掀起了一场巨大的革命, 传统企业也加入了深度学习的浪潮, 计算机视觉、模式识别和自然语言处理的变化超出了人们的想象。近年来, 计算机视觉和模式识别取得了很大的进展。但由于人与人之间的差异、文化的差异以及人们对自然语言的理解, 自然语言处理还存在着一些复杂的问题。自然语言处理领域一直面临着复杂的问题。NLP<sup>[1]</sup>起源于20世纪40年代。起先的工作运用了语言学理论并利用计

算机对自然语言进行理解, 从而对自然语言进行处理。在自然语言领域中, 目前发展比较快的一些任务有机器翻译、机器理解和问答系统。

问答系统的一般业务流程是在用户输入一个问题后, 系统需要根据问题找到最合适的答案。问答系统旨在自动找到任何问题的答案。传统的研究使用浅层概率对问题和答案进行分类, 如果某个句子与其中一个问题非常匹配, 这个句子就是那个答案。几十年来, 机器学习(支持向量机、贝叶斯分类等)成为问答系统的实现方式。

收稿日期: 2019-06-29

修回日期: 2019-10-30

网络出版时间: 2019-12-18

基金项目: 国家自然科学基金(61773384)

作者简介: 王乾铭(1995-), 男, 硕士研究生, 研究方向为知识图谱、自然语言处理; 李 吟, 博士研究生, 工程师, 研究方向为大数据、知识图谱、人工智能。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20200110.1118.016.html>

传统的 seq2seq 模型中的输出结果往往是在输出之前选出出现概率最大的单词,也即极大似然估计。而训练语料中,作为结果输出的单词可能在训练语料中的出现概率就很大,比如“ok”、“yeah”、“I’m sorry”这类携带信息较少而出现比较频繁的单词,这样就会导致极差的用户体验。一个吸引人的反应生成系统应该能够输出语法上的、连贯的、多样的、有趣的反应。因此文中使用 Beam Search 这种启发式搜索算法,它不同于传统的贪婪算法,可以输出概率最大的若干个句子,从而增加回复的多样性和趣味性。

对于传统的 seq2seq 模型的问答系统还存在一个普遍的不一致性问题。由于利用深度学习训练问答机器人时,都会使用大量的语料,而一般常见的问答语料,例如美国康奈尔大学搜集的电影对话语料“Cornell Movies-Dialogs Corpus”或者大型开放字幕库“Open Subtitles”以及 Ubuntu 社区问答语料“Ubuntu Corpus Dialogs”,都有着覆盖面广、开放式、有噪声的特点。如图 1 所示,利用这些语料直接训练的问题就是同样意思但不同表达的问句会得到不同答案。这就影响了问答机器人的效果以及使用功能。而文中利用不同语料多次训练的方式能够克服这个问题,从而得到良好的效果。

---

Q: who are you ?  
A: I am the bowler.  
Q: What's your name ?  
A: Laure.

Q: Where do you live now?  
A: I live in Los Angeles.  
Q: In which country do you live now?  
A: England, you?

---

图 1 一般问答机器人的不一致性问题

## 1 相关工作

问答系统可以追溯到艾伦·图灵的图灵测试。用户输入问题,然后模型给出相应的准确答案。1980 年至 1991 年,对知识库的问答系统进行了研究,但大部分知识库相对有限,没有太多的参考价值。在 1991-1999 年,行业内普遍使用统计建模和机器学习来构建问答系统。而问答系统被认为是最接近人工智能的产品。10 年后,Siri 的出现对问答系统来说具有跨时代的意义。如今,随着数据的快速发展,传统的搜索系统如谷歌和百度,它们的算法已经不能满足人们的要求。因此,他们试图选择问答系统作为一种新的方式来完成客户的需求。

对于问答系统,学术界的研究主要有三种类型:

(1)统计句子字数的方法<sup>[2]</sup>。根据问题统计频率的接近性,得到与问题相对接近的答案的频率。但是仅仅使用统计知识并不能很好地理解客户。比如知识检索图书馆系统。

(2)机器学习<sup>[3-4]</sup>。他们用概率和统计的方法构建了问答系统。就像 SVM,k 均值算法。这些机器学习算法利用数据样本的特征值,将这些特征组合成矩阵作为模型的输入。

(3)深度学习<sup>[5-7]</sup>。深度学习技术可以有效地减少数据集的创建和预处理时间。此外,它还可以减少人为因素造成的误差。最后,它显示了比以前更好的结果。特别是在大数据集中,深度学习比其他方法更有效。而且它不需要手动提取特性,所以实现起来很简单。深度学习算法在自然语言领域的第一个应用是 CNN。在 CNN 的汇聚效应下,有效地减少了数据的浪费,准确地获得了相应的参数数据。

利用深度学习技术使自然语言处理领域的问答系统得到了飞速发展。使用 RNN 技术的聊天机器人模型可以不需要预定义一个知识库,它可以直接生成答案<sup>[8-12]</sup>。这种方法的思路来自于自然语言领域中的机器翻译技术。Ritter 等<sup>[8]</sup>使用了大规模微博聊天数据集进行训练,并将问题当作翻译中的源语言,答案当作翻译后的目标语言,从而将机器翻译的技术运用到了问答上。Hinton 等<sup>[9]</sup>提出了一种自动编码器,Cho 等<sup>[10]</sup>设计了一种新的对 RNN 进行改进后的 GRU 网络。Shang 等<sup>[11]</sup>在此基础上同样使用大量的微博对话数据集训练出了一个基于 Sequence-to-Sequence 框架的 RNN 网络。谷歌提出的神经会话模型<sup>[12]</sup>,利用了 4 种不同的数据集对 Seq2Seq 模型进行训练。文中正是在这个模型的基础上进行改进。

## 2 模型构建

文中模型是在 Seq2Seq 架构的基础上进行改进的。Seq2Seq 是一种典型的基于编解码器的体系结构。该架构最初出现在机器翻译领域,由 Cho 等人在 2014 年 EMNLP 会议<sup>[10]</sup>上提出。经过 Liu 等人的升华,出现了 Seq2Seq<sup>[13-14]</sup>模型。Seq2Seq 主要由编码器、解码器和状态向量组成。Seq2Seq 的基本架构如图 2 所示。

编码器:编码器的作用是转换输入变长序列成定长状态向量,状态向量包含有关输入序列的信息。

状态向量:状态向量是由编码器的隐藏层向量决定的,它将输入序列的信息从编码器发送到解码器。

解码器:解码器通过对状态向量和前一时刻解码器的输出向量进行解码,从而能够生成可变长度的序列。

编码-解码器体系结构在一定程度上简化了数据集,将数据集转换为固定长度向量通过编码器表示,且向量作为数据集引入网络进行训练。该解码器对算法的输出进行解码,解码的思想是用概率论的方法输出不确定长度的答案。这样的体系结构提高了系统的效率和精度,使其特别适用于自然语言处理任务。

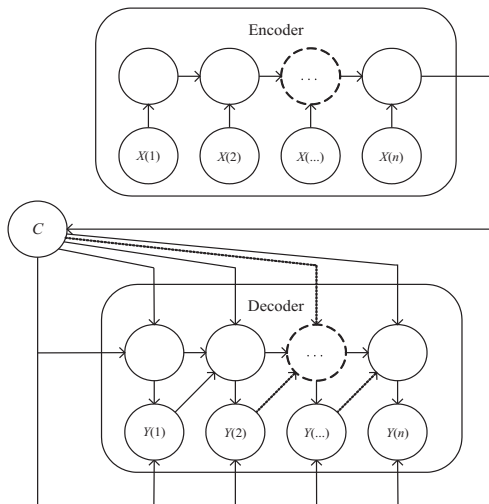


图2 Seq2Seq 基本结构

文中使用 LSTM(long short term memory)<sup>[15-17]</sup> 结构作为 Seq2Seq 模型中提取句子信息的单元结构。LSTM 是一种循环神经网络模型。循环神经网络利用前一个节点的反馈作为输入,利用递归思想迭代映射输入和参数,计算输出和损失,然后进行循环计算形成动态网络。

LSTM 网络是 RNN 的一种变体,是一种更实用、更极端的变体。LSTM 网络是一种能够在自循环下产生长时间连续流梯度的结构。LSTM 对消失梯度和非自然梯度下降具有良好的适应性。

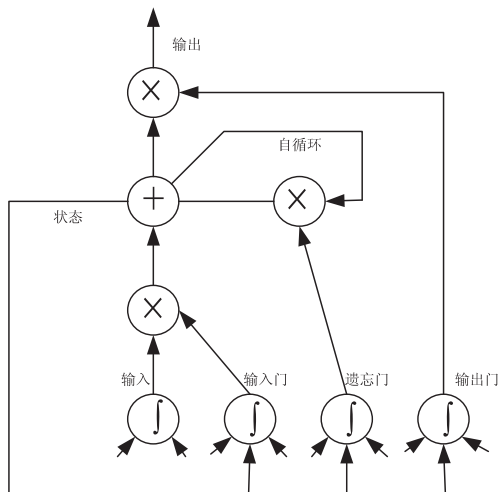


图3 LSTM Cell 结构

首先,它选择单元格来代替门的描述。然后,每个细胞之间相互连接,而不是直接利用一般神经网络的隐藏单元。由图3可知,输入门的数据和输入数据要

进行计算,遗忘门从状态量中修正向量,并且它也加入了自循环。在自循环的同时,状态返回向量到输入门、遗忘门和输出门。每个门都根据状态给出的值进行调整。最后输出门和状态影响输出。激活函数选择 Sigmoid 函数。上述过程的公式如下:

$$\text{forget}_i^t = \sigma(b_i^f + \sum_j U_{i,j}^f x_j^t \sum_j W_{i,j}^f h_j^{t-1}) \quad (1)$$

其中,  $t$  是当前的 epoch 值,  $x^t$  是输入向量,  $h^t$  是输出的最终结果,  $b^f$ ,  $U^f$ ,  $W^f$  是偏置参数,输入权重矩阵和向量矩阵。遗忘门被用来表示循环权向量的状态量。它的权重随着状态有一定的更新。

自循环权矩阵的更新公式如下:

$$\text{Selfloop}_i^t = \text{forget}_i^t \text{Selfloop}_i^{t-1} + \text{input}_i^t \sigma(b_i^g + \sum_j U_{i,j}^g x_j^t \sum_j W_{i,j}^g h_j^{t-1}) \quad (2)$$

输入门的更新公式如下:

$$\text{input}_i^t = \sigma(b_i^g + \sum_j U_{i,j}^g x_j^t \sum_j W_{i,j}^g h_j^{t-1}) \quad (3)$$

同时需要给输出一些限制,最后选择了 tanh 函数作为激发函数:

$$h_i^t = \tanh(S_i^t) \text{outgate}_i^t \quad (4)$$

$$\text{outgate}_i^t = \sigma(b_i^o + \sum_j U_{i,j}^o x_j^t \sum_j W_{i,j}^o h_j^{t-1}) \quad (5)$$

总之,LSTM 可以解决长依赖的问题,可以记住并学习更多的知识。而多层的 LSTM 结构往往比单层结构的效果更好,因此文中采用了 4 层的 LSTM 结构。

Seq2Seq 模型中用一个固定长度的向量编码了所有输入序列的语义信息,限制了模型性能的提高,注意力机制(attention mechanism)则允许模型自动搜索源输入序列中与目标序列词汇相关的部分信息,注意力机制可以使得输出的结果能够关注不同的输入。在没有注意力机制之前,当输入序列的句子比较长,原始的 Seq2Seq 模型只用一个中间语义向量来表示所有的输入序列的语义,这就会导致丢失很多输入序列的细节信息。注意力机制的结构如下:

在编码器-解码器结构中,最后解码器的输出层根据输入序列  $X$  预测单词的概率是:

$$P(y_i | y_1, \dots, y_{i-1}, x) = g(y_{i-1}, s_i, c_i) \quad (6)$$

其中,  $s_i$  是 RNN 在时刻  $i$  的隐层状态,  $s_i$  的计算公式为:

$$s_i = f(s_{i-1}, y_{i-1}, c_j) \quad (7)$$

对于输入序列的状态  $h_i$ , 此处引入不同的权重:

$$c_j = \sum_{k=1}^{T_s} \alpha_{i,j} h_{j,k} \quad (8)$$

权重的计算公式是:

$$\alpha_{i,j} = \frac{\exp(e_{i,j})}{\sum_{k=1}^{T_s} \exp(e_{i,k})} \quad (9)$$

其中,  $e_{i,j}$  是由输入序列的状态决定的,计算公式

如下：

$$e_{i,j} = V^T \tanh(W_1 h_j + W_2 s_{i-1}) \tag{10}$$

文中的 Seq2Seq 模型是在传统的 Seq2Seq 模型的基础上进行了改进,采用 4 层的 LSTM 结构<sup>[18]</sup>并且增加了注意力机制,如图 4 所示。使用多层的 LSTM 结

构能增加整体的参数量,这使得编码器能够更加精准地提取输入序列的语义信息。从图中看,其中最主要的改进就是在 Seq2Seq 模型的 Decoder 过程中每个输出都可以得到一个结合输入状态的权重。这样输出的单词会更准确,或者在含义上能够更符合问句。

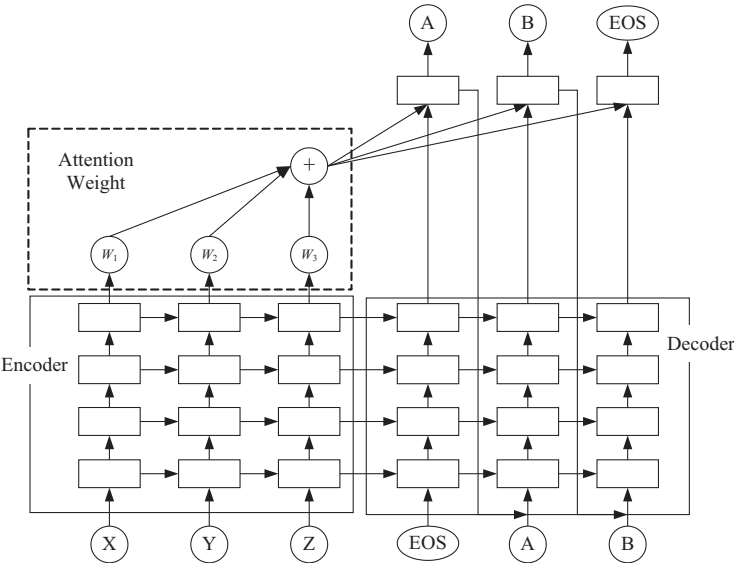


图 4 改进后的 Seq2Seq 模型的结构

传统的 Seq2Seq 模型在解码过程中采用的是 Greedy Search, Greedy Search 本质上是一种贪心算法,在解码过程中每一个单词的输出都选择了概率最大的值,然后将这个值作为下一个时刻的输入。最终得到的结果经常会出现重复的安全回复,因为在训练集中例如“I don’t know”等等出现的次数比较多。Beam Search 算法则是在解码过程中首先输出概率最大的前 K 个单词,然后再将这 K 个单词分别作为输入计算它们下一时刻的输出,最终能得到 K 个结果。所以系统的回复就能够变得更多样化。

3 系统的设计与实现

3.1 数据集

文中使用的数据集是康奈尔大学搜集的电影对话语料“Cornell Movies-Dialogs Corpus”,该数据集共包含 10 292 对电影人物之间的 220 579 次会话交流,涉及 617 部电影中的 9 035 个角色,总共 304 713 条话语。所以将其中的 200 579 条数据用于训练,其他的 20 000 条数据用于测试。

文中采用的一个数据集就是生活大爆炸的台词对话语料。为了给问答机器人赋予一个角色,使其有一定的个性化,选取了 Sheldon 与其他人的对话,具体就是将原来的数据集进行过滤,最终只保留 Sheldon 回答其他人的对话,具体信息如图 5 所示。该数据集共包含了 50 685 条对话。其中 45 685 条数据用于训练,5 000 条数据用于测试。

Penny: Well imagine how I’m feeling.  
Sheldon: Hungry? Tired? I’m sorry this really isn’t my strong suit.  
Leonard: You told her I lied, why would you tell her I lied?  
Sheldon: To help you.

图 5 《生活大爆炸》对话语料

3.2 数据处理与模型实现

文中的代码实验利用了谷歌的 Tensorflow 框架,第一步先分析两种数据集,通过对文件进行处理生成.pkl 格式的数据集,然后根据 Tensorflow 框架中的 Seq2Seq 框架去定义网络的输入值。

(1)编码器的输入:第一个角色说的句子 A,并且设定了句子 A 的最大长度为 10 个单词。

(2)解码器的输入:第二个角色回复的句子 B,因为前后分别加上了 go 开始符和 end 结束符,最大长度为 12。

(3)解码器的目标输入:解码器输入的目标输出,与解码器的输入一样但只有 end 标识符号,可以理解为解码器的输入在时序上的结果,比如说完这个词后的下个词的结果。

(4)解码器的权重输入:用来标记 target 中的非 padding 的位置,即实际句子的长度,因为不是所有的句子的长度都一样,在实际输入的过程中,各个句子的长度都会被用统一的标识符来填充(padding)至最大长度,weight 用来标记实际词汇的位置,代表这个位置将会有梯度值回传。



最终计算 Softmax Loss, Softmax Loss 是一种交叉熵损失函数,它的具体形式是:

$$E(t,y)=-\sum_i t_i \log y_i$$

(11)

$$y_i = \text{softmax}(z_i) = \frac{e^{z_i}}{\sum_i e^{z_i}}$$

(12)

3.3 模型训练及结果分析

文中的训练及测试在一台 GPU 服务器上完成。GPU 服务器的配置见表 1。

表 1 GPU 服务器配置

硬件名称	配置
CPU	至强 E5-2600v4
内存	32g
GPU	NVIDIA TITAN V
显存	12G

训练时采用基于 Adam 算法的随机梯度下降算法,学习率是 0.002,每个 batch 包含 256 个问答对。另外利用了 Dropout 技术来避免出现可能的过拟合问题,Dropout 的比率设为 0.1。

模型的训练分为两个阶段。第一个阶段将两个数据集同时进行训练,一共训练 90 个 Epoch,这一阶段的训练是为了使系统覆盖的知识面更广。第二阶段就是只用 Sheldon 数据集进行训练学习,一共训练 30 个 Epoch。

文中最终训练了两个模型,一个是只利用了传统的 Seq2Seq 结构,一个利用了 Seq2Seq 结构加上注意

力机制。  
实验过程记录的损失函数曲线如图 6 所示。

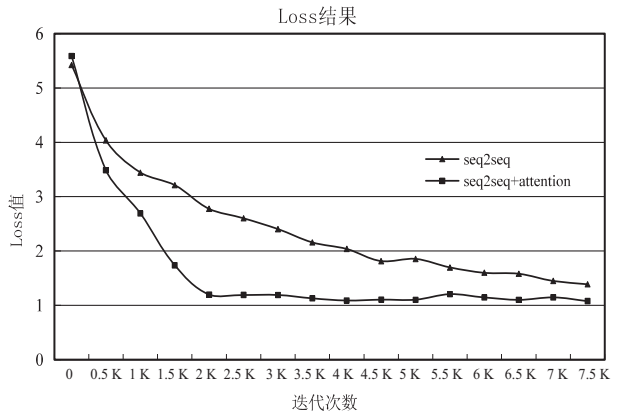


图 6 两种模型的 loss 曲线对比

结果显示:增加了 attention 机制的模型 loss 值比原模型下降的快,这有助于模型能够快速收敛到稳定值,并且最终的 loss 值也比原模型要低。

为了更精确地测试两模型的区别,文中引入了两个自动评估指标:BLEUs<sup>[19]</sup>、Distinct-n。

BLEUs 指标是从机器翻译中的评估指标引申过来的,它是通过判断回复句子和参考回复句子的词汇重叠度来表示回复的质量。

针对对话系统中万能回复的问题,通过计算生成回复中 1 元词和 2 元词的比例来衡量回复的多样性。具体来说,Distinct-1 和 Distinct-2 分别是不同的 unigrams 和 bigrams 的数量除以生成的单词总数。

评估结果如表 2 所示。

表 2 三种评估指标结果

模型	BLEU-1	BLEU-2	BLEU-3	BLEU-4	Distinct-1	Distinct-2
Seq2Seq( Baseline)	0.367	0.122	0.055	0.028	0.021	0.072
Seq2Seq+Attention	0.439	0.274	0.083	0.056	0.029	0.096
Seq2Seq+Attention+ Beam Search	0.257	0.098	0.042	0.019	0.043	0.147

从实验结果可以看出:加入了注意力机制后,三个指标较原来的模型都有提高。当在测试时加入了 Beam Search 算法时,回复的多样性有了明显的提高。但是 BLEU 指标与原来的相比有所下降,原因是 BLEU 指标只专注于句子之间词汇的重复率,当增加了回复的多样性之后,回复的句子就会常有相同意思

但不同的表达,这就会减小回复句子与目标句重复单词的概率,因此 BLEU 指标会有所下降。下面通过输入一些问句,将它与原有模型进行对比,去测试系统的一致性以及是否具有角色的个性。

表 3 是测试了若干组问句抽出的几个结果。

表 3 两种模型测试问句结果

问句	传统模型的回复	文中模型的回复
What's your name?	Laure.	I'm Sheldon.
who are you ?	I am the bowler.	Sheldon.
What do you want?	I am not sure.	I want to talk to you.
What for?	Nothing.	I have to go to the bathroom.

续表 3

问句	传统模型的回复	文中模型的回复
what do you think?	Ask him.	It's so simple.
Tell me something?	Punk rock is over.	No, It's my secret.
What's your mean?	Nothing.	Oh, I am getting too much for you .

从结果可以看出,新模型的回复有了一定的一致性,相比于传统模型,回复质量有了一定的提高,回复的语句也比原来更流畅,效果更好。

4 结束语

通过对 Seq2Seq 模型进行了改进,针对一般问答机器人的一致性和多样性的问题进行改进,训练出了一个个性化的问答机器人,和原有模型相比提高了一定的回复质量,并且在 BLEUs 和 Distinct-n 指标上做了相应的测试,也都获得了不错的结果。对于未来的工作,准备将问答机器人和知识库相结合,使它在遇到不知道的问题时能够从本地知识库搜索,或者从网络上利用搜索引擎进行查找,从而进一步增强问答机器人的作用,提高其回复质量。

参考文献:

[1] 袁琦. 中文信息技术和自然语言处理[J]. 中文信息学报,1986(1):33-36.

[2] YOUNG S,GASIC M,THOMSON B,et al. POMDP-based statistical spoken dialog systems;a review[J]. Proceedings of the IEEE,2013,101(5):1160-1179.

[3] JOACHIMS T. Text categorization with support vector machines;learning with many relevant features[C]//Proceedings of the 10th European conference on machine learning. Berlin;Springer,1998:137-142.

[4] AIKAWA N,SAKAI T,YAMANA H. Community QA question classification;is the asker looking for subjective answers or not? [J]. IPSJ Online Transactions,2011,4:160-168.

[5] 孙志军,薛磊,许阳明,等. 深度学习研究综述[J]. 计算机应用研究,2012,29(8):2806-2810.

[6] 孙志远,鲁成祥,史忠植,等. 深度学习研究与进展[J]. 计算机科学,2016,43(2):1-8.

[7] 王龙,杨俊安,陈雷,等. 基于循环神经网络的汉语语言模型并行优化算法[J]. 应用科学学报,2015,33(3):253-261.

[8] XU Anbang,LIU Zhe,GUO Yufan,et al. A new Chatbot for customer service on social media[C]//Proceedings of the

2017 CHI conference on human factors in computing systems. New York,NY;ACM,2017:3506-3510.

[9] HINTON G,KRIZHEVSKY A,WANG S. Transforming auto-encoders[C]//Artificial neural networks and machine learning (ICANN). Berlin;Springer,2011:44-51.

[10] CHO K,VAN MERRIËNBOER B,GULCEHRE C,et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation[C]//Empirical methods in natural language processing. Stroudsburg, PA: ACL, 2014: 1724-1734.

[11] SHANG Lifeng,LU Zhengdong,LI Hang. Neural responding machine for short-text conversation[C]//Proceedings of the 53rd annual meeting of the association for computational linguistics and the 7th international joint conference on natural language processing. Stroudsburg, PA: ACL, 2015: 1577-1586.

[12] DALE R. The return of the chatbots[J]. Natural Language Engineering,2016,22(5):811-817.

[13] 刘洋. 神经机器翻译前沿进展[J]. 计算机研究与发展, 2017,54(6):1144-1149.

[14] ZHANG Yong,XIAO Weidong. Keyphrase generation based on deep Seq2seq model[J]. IEEE Access,2018,6:46047-46057.

[15] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Neural Computation,1997,9(8):1735-1780.

[16] SUNDERMEYER M,NEY H. From feedforward to recurrent LSTM neural networks for language modeling[J]. IEEE/ACM Transactions on Audio Speech & Language Processing, 2015,23(3):517-529.

[17] GERS F A, SCHMIDHUBER J, CUMMINS F. Learning to forget;continual prediction with LSTM[J]. Neural Computation,2000,12(10):2451-2471.

[18] 刘腾飞,于双元,张洪涛,等. 基于循环和卷积神经网络的文本分类研究[J]. 软件,2018,39(1):64-69.

[19] PAPINENI K,ROUKOS S,WARD T,et al. BLEU;a method for automatic evaluation of machine translation[C]//Proceedings of the 40th annual meeting on association for computational linguistics. Philadelphia;Association for Computational Linguistics,2002:311-318.