|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. 发明人信息 (如存在外籍发明人需要特别指出，每个发明人的贡献比例将等同于奖励比例) | | | | |
|  | 发明人 | 贡献比例 | 联系方式(手机+邮箱) | 部门 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 1. **发明完成日期** | | | 具体技术完成时间2021年10月8日 | |
| 1. **发明完成地点** | | | 电子科技大厦 | |
| 1. **第一发明人身份证号码** | | |  | |
| 1. **技术支持人 姓名、电话及邮箱** | | |  | |
| 1. **方案名称** | | | | |
| **通过监督对比学习改进文本分类** | | | | |
| 1. **是否为在研的研发项目，项目名称为？预计上线时间？** | | | | |
| **否** | | | | |
| 1. **之前是否递交过跟该项目相关的技术交底书，或者与该技术交底书相关联的其他交底书（例如某一技术交底书的方案更新版）？技术交底书名称是？** | | | | |

|  |
| --- |
| **否** |
| 1. **背景技术(必填项)** |
| 请用简洁的语言说明该发明所属的技术领域或者直接应用的技术领域；  详细介绍一下与本发明专利申请要求保护的主题相关的现有技术的现状、工作原理、工作方式如何？客观地指出现有技术的缺点和不足，解释一下原因。  **所属的技术领域**：  自然语言处理  **现有技术现状**：  对比学习是一种判别式自监督学习方式，通过预先制定的数据转换策略，自动构造相似样本与不相似样本，然后利用对比损失函数，拉近相似样本(正样本)的距离同时推开不相似样本(负样本)之间的距离。这种训练方式已经被广泛的应用在CV和NLP领域以获取高质量的向量表示空间，取得的优异成绩吸引了极大的关注度。基于对比学习的模型有两个重要的部分：一个是数据转换策略，有效的数据转换策略可以决定最终所学习到的向量表示的不变性，提高表示向量在下游任务的表现，目前在NLP领域，常用的数据转换策略包括：插入、删除单词，单词顺序打乱以及其它的比较简单、浅层的方法。另一个就是对比损失的设计，实践表明，增加负样本的数量可以提升最终表示空间中表示向量的质量。然而在NLP领域，目前常用的基于对比学习的文本表示模型大多采用端到端的结构，而这种结构增加负样本就等同于增加同一批次的训练样本数量(batch)，显然要受到显存限制，另一方面研究表明，简单的增加batch的大小甚至还会降低句向量的质量。此外，目前大量的研究(尤其是NLP领域)主要集中于以自监督的方式应用对比学习，而很少在有监督任务上融入对比学习的思想。  **现有技术缺点：**   1. 数据转换方面。在NLP领域，目前流行使用的数据转换方式包括：随机删除、插入，或者利用网络中的dropout机制作为数据增强策略，然而每一种方法都有各自的问题。比如随机删除单词的方式有可能会删除体现整个句子语义的单词，从而改变原始句子的语义。此外，dropout机制尽管简单有效，但是研究表明，由于dropout策略没有改变句子长度，所以句子的长度信息会作为一种特征来区分正负例，使得模型偏向将长度一致的句子视为正例，将长度差异较大的句子视为负例。 2. 损失函数方面。对于第，对比损失函数的设计包括一个正样本和个负样本。批次的大小。在基于端到端的结构中，这种对比损失函数的设计目前只包含一个正样本，而且受到显存限制以及其它因素，不能增加负样本的数量。此外自监督的方式不可避免的会采样到与原始句子实际上语义相似的句子作为负样本，不利于学习向量表示。 3. 目前NLP领域的研究主要集中于以自监督的方式进行对比学习训练句向量，而很少将对比学习用在有监督任务上作为一种辅助任务提高模型有监督任务上的表现。 |
| 1. **设计要点(必填项)** |
| 针对现有技术的缺点和不足，阐述本发明的发明目的、解决的技术问题是什么？要达到的效果是什么？  为了解决现有问题的不足，请用技术的语言简要列出本发明的设计要点，即：本方案必须具备的技术点，以及每个设计要点所起的作用和达到的效果。  本发明要解决的技术问题&要达到的效果：   1. 利用对抗样本作为数据增强的策略，提高正样本的质量，避免简单的随机插入、删除单词操作可能带来的句子语义改变等问题。 2. 将对比学习以监督的方式作为辅助任务应用在监督任务上，提高模型在监督任务上的表现。同时利用监督任务中的标签信息作为额外的学习信号，改进对比损失函数，提高最终学习的句向量的质量。 3. 利用动量对比机制实现在不扩大批次大小的前提下增加负样本数量，目标仍然是提高最终学习的句向量的质量。   发明设计简要说明：   1. 对抗样本的生成可以采用黑盒攻击技术，如TextFooler方法，将带有类别标签的句子输入到模型中，通过同义词替换等操作重复的输入给模型，在不改变句子语义的前提下直到模型预测类别错误或者输出较低的置信度为止。 2. 在自监督形式的对比损失函数中，对于某一个句子，通常将一个批次内的其余所有句子作为负样本推开它们在表示空间中的距离。然而在一个批次内很多个句子会同属于一个类别，推开同一类别内的句子之间的距离会降低模型分类的准确率。因此采用监督形式的对比损失，即利用监督任务的标签信息。具体来说，对于某一个句子，会将这个批次内和这个句子同属于一个类别的所有句子作为这个句子的正样本，将其余类别的句子作为负样本。因此监督形式的对比损失不同于自监督形式，一个原始样本会有多个正样本。 3. 动量对比机制主要包含一个队列和一个缓慢更新的编码器。其中队列保存的是每一批句子的句向量以及该句子对应的类别，编码器采用对抗样本阶段使用的黑盒模型，因为该模型已经具有一定的容错性，对一些对抗样本更加的鲁棒。 |
| 1. **具体实施方式(必填项)** |
| 结合具体实施例和附图，完整、清楚地写出本发明要实现上述发明目的的具体技术方案，使本领域的普通技术人员能够理解该技术方案，并能按照该技术方案实现本发明的发明目的。本部分非常重要，这是发明专利的核心部分。  **对于一种XXX装置的专利申请来说**，要结合图纸详细说明构成本发明XXX装置都有哪些部分？各部分的连接关系？位置关系？实现发明目的的工作原理。  **对于一种XXX方法的专利申请来说**，要结合反映该方法的程序框图、按照时间顺序详细说明具体的实现步骤，在描述该方法时，要将一切条件、数据、材料、设备、工具和必要的技术规格、型号等进行必要的交代，使同领域的普通技术人员能够按照您的说明，将该发明或者实用新型再现出来，而不能建立在自己已经深刻理解本方案的前提下。 1. 公式/符号说明.    |  |  | | --- | --- | | **公式/符号** | **含义** | | [CLS] | 一个特殊的字符，添加在输入句子的第一个单词之前，编码后的向量表示整个句子的语义。 | |  | 一个批次中数据的个数。 | |  | 动量对比机制中所用队列的容量。 | |  | 对比损失函数中的一个重要参数，称为温度系数。 | |  | 第个句子经过BERT的编码向量。 | | BERTa | 生成对抗样本所使用的编码器，经过对抗训练后，BERTa同样还会作为动量对比阶段所使用的动量编码器。 | | BERTc | 监督任务中的编码器，同时进行句向量表示学习和分类任务。 | |  | 第样本的监督对比损失(Supervised Contrastive Loss) | |  | 向量向量余弦相似度，计算公式： |  2. 通过监督对比学习改进文本分类 2.1 相关工作  相关工作包括：预训练语言模型、对抗样本、对比学习等。  预训练语言模型（比如BERT）已经在各种NLP任务上达到了显著的效果，是最为常用的编码器。目前仅利用BERT自身就可以在文本分类等任务上表现出惊人的成绩，利用BERT做文本分类任务时，一般取最后一层第一个位置的字符(即[CLS])对应的向量作为整个句子的语义表示进行分类。如下图1所示。    图1. 利用BERT进行文本分类  对抗样本最初用在CV领域，指的是那些经过数据处理操作后的图片，与原始图片相比人眼观测不出变化却能够使得模型发生误判的样本。而在NLP领域，由于句子是由单词构成的，这种离散性使得稍微的改变部分单词就会被人眼发觉，因此NLP领域的对抗样本指的是经过数据处理操作后的句子，与原始句子相比语义并未改变，却能够使得模型发生误判的句子。生成对抗样本的方式分为白盒攻击和黑盒攻击。白盒攻击的策略需要根据标签计算模型参数的梯度，沿着梯度上升的方向添加扰动再降低损失。本文采用黑盒攻击策略，不关系模型具体参数等细节，而是通过同义词替换等操作在尽可能不改变原始句子语义的前提下更改句子，使得模型发生误判。目前比较流行的黑盒攻击方法有TextFooler等，如下图2所示：    图2. TextFooler方法。原始句子预测为消极类别，通过同义词替换操作改变原始句子，模型预测为积极类别。  自监督学习属于无监督学习的一种，通过预先制定的辅助任务从无标注数据中训练模型学习有效的向量表示，预训练好的模型供下游任务使用，可以极大的提升模型在下游任务上的表现。这种训练机制已经被广泛的应用在各个领域。常见的辅助任务如文本领域的掩码语言模型任务，该任务属于生成式自监督学习，通过在输入上添加噪声让模型重构原始输入，或者图像领域的角度预测任务，该任务属于判别式自监督学习，让模型预测一幅图片被旋转的角度，这个角度就是大多数判别式自监督学习任务需要的伪标签。最近，一种判别式自监督学习方法(也称为对比学习)由于其在CV和NLP领域取得的优异成绩吸引了极大的关注。与上述的自监督学习任务不同，既不需要伪标签，也不像生成式自监督学习需要重构原始输入，对比学习的思想是通过对比输入的样本进而学习一个表示空间，在这个表示空间中，相似样本的距离很近，不相似样本之间的距离较远。具体来说，对比自监督学习的目标是首先利用数据转换策略生成原始输入数据转换后的版本，随机从原始数据中挑选一个样本，从转换数据中挑选一个样本，让模型预测这两个样本是否来自于同一个原始数据(或者说其中一个样本是否是另一个样本经过数据转换得到)，如下图3所示。    图3. Transformation代表数据转换模块。Encoder代表编码模块。相似样本指的是一幅图片经过数据转换后的图片，不相似样本指的是其它图片。  基于对比学习的网络结构目前有很多种，根据负样本的采集过程不同可以大致分为四类结构：端到端形式；使用内存池；使用动量编码；引入聚类。在CV领域，以上四种架构都有各自的优势，而在NLP领域，目前最常使用的是基于端到端(end-to-end)的结构。此外在CV领域，常用的数据转换包括旋转、裁剪等，而在NLP领域，目前常用的数据转换包括回译、随机插入(insert)或删除(delete)单词等。目前NLP领域基于对比学习的表示模型结构大致如下图4：    图4.基于对比学习的文本表示模型结构  其中对比学习的损失函数(contrastive loss)一般采用如下公式：    其中代表输入的样本个数(例如图4中=2)，代表两个向量的相似性，一般采用余弦相似性度量。代表第个句子经过BERT编码得到的句向量，代表第个句子经过插入和删除等数据转换操作得到的句子对应的句向量。对比学习的思想就是将这两个句子视为正样本拉近它们在表示空间中的距离，同时推开第个句子与其它句子的距离。  2.2 模型结构  整体的结构如图5所示。接下来将根据发明设计简要说明中提出的三部分依次阐述模型结构。  首先是TextFooler模块。由于简单的随机插入删除等数据增强操作可能会改变原始句子的语义信息，因此本文采用对抗攻击与防御领域中的一种数据增强方法textfooler。攻击的模型采用BERT(图中并没有展示textfooler内部具体细节，后续将textfooler中的BERT命名为BERTa)，攻击方式为黑盒攻击。具体来说，首先利用原始的分类数据微调BERTa，使得BERTa可以学习到分类数据的特征。然后将每一个句子再次输入BERTa，在模型预测正确的前提下通过同义词替换等操作改变句子结构，重新输入BERTa直到预测错误为止。此时的句子可以作为原始句子的对抗样本。(如果始终无法使得模型预测错误，那么选择模型输出置信度最低的那个版本的句子作为对抗样本。)将上述操作生成的对抗样本加入训练集进一步微调BERTa，增强模型的鲁棒性。    图5. 从Cross-Encoders到Bi-Encoders的注意力蒸馏结构  其次是动量编码(momentum encoder)模块。该模块通过缓慢更新的方式使得队列中保存的多个批次的句向量保持了一定程度上的一致性。该模块的编码器采用TextFooler模块中经过对抗训练后的BERTa，将当前批次内生成的对抗样本输入到动量编码器中，编码的向量存储在队列中，如果队列达到最大容量，则移除之前批次放进去的句向量。此外，由于本文采用有监督形式的对比学习，所以还需要保存每一个句向量所对应的句子的类别。  最后是对比损失函数的设计。自监督形式的对比损失中正样本来源于数据增强后的样本，负样本是从当前批次的所有数据增强后的样本或者数据集中随机挑选样本得到的。这并不适用于监督任务，因为一个批次内势必会包含同一类别的很多样本，特别是当类别数目少而且批次数量大的情况下。监督形式的对比损失中，负样本取自同一批次下与该样本属于不同类别的样本，为了增加正样本的数量，可以将与该样本属于同类别的其他样本均作为正样本。此外，通过利用动量对比机制，可以进一步增加正样本和负样本的数量。最终的对比损失函数的设计如下公式：  C:\Users\User\AppData\Local\Temp\1633576193(1).png  其中表示与当前的句子属于同一类别时取值为1，不同类别取值为0。分别是批次的大小和队列的容量，当前批次和队列中与句子属于同类别的样本数量。因此对于第个样本的对比损失，其含义为将当前批次以及队列中所有和其同类别的样本作为正样本拉近同类别样本之间的距离，其余不同类别的样本作为负样本，推开不同类别样本之间的距离。(需要注意的是，队列中的向量是经过BERTa编码得到的，而当前批次的样本是输入到BERTc中编码。所以两者的向量表示有差异，不过公式中统一用表示。) |
|  |

|  |
| --- |
| 1. **技术效果**   本方案达到的技术效果：   1. 将对比损失以监督的形式应用在文本分类任务上，使得模型可以学习到不同类别的样本表示特征之间的差异，进而提高分类准确率。而且最终的模型既可以用来做分类任务，也可以做语义匹配任务。 2. 通过引入对抗样本、动量对比等机制，提高最终学习的文本表示质量。 |
| 1. **请将填写好的技术交底书提交至大为专利管理系统，网址**[**http://10.26.24.36/，并通知**](http://10.26.24.36/，并通知)**于立群。** 2. 若发明已被披露或于未来30天内将被披露给销售商、供应商或消费者，请尽快通知IP部加急处理。 3. 未来是否有披露计划？如有，请指明计划披露日期和对象，包括将向其披露该发明的制造商、销售商、承包商、放款人等，无论是否已签订NDA。 4. 如发现近似专利、论文文献请提供。 5. 如有能够帮助相关人员理解本发明的其他技术参考文献请提供。 |