|  |  |
| --- | --- |
| 编 号 |  |
| 密 级 |  |
| 阶段标记 |  |
| 页 数 |  |

|  |  |
| --- | --- |
| **名 称** | **提示学习调研任务** |

|  |  |
| --- | --- |
| 会 签 | |
|  | |
|  |  |
|  | |
|  |  |
|  | |
|  |  |

|  |  |
| --- | --- |
| 单 位 |  |
| 编 写 |  |
| 校 对 |  |
| 审 核 |  |
| 标 审 |  |
| 批 准 |  |

**中国科学院空间科学与应用总体部**

年 月 日

目录

[1 提示学习简介 1](#_Toc109035602)

[2 提示学习相关研究 1](#_Toc109035603)

[2.1 提示学习影响因素 1](#_Toc109035604)

[2.2 prefix-tuning影响因素 3](#_Toc109035605)

[2.3 LM阶段和提示学习阶段的不平衡问题 3](#_Toc109035606)

[2.4 提示学习模板构建和使用方式 4](#_Toc109035607)

[2.5 soft prompt 4](#_Toc109035608)

[2.6 动态提示+静态提示 4](#_Toc109035609)

[2.7 稳健性研究 5](#_Toc109035610)

[2.8 损失函数、分值计算等方面的改进 5](#_Toc109035611)

# 提示学习简介

提示学习是尽可能的将下游任务建模为PLM（pretrain language model）的任务范式，以实现在低数据资源下完成下游任务。

提示学习的过程，大致分为三步：

1. 针对任务目标，建立提示模板。
2. 答案搜索，填充模板中的[mask]位置。
3. 答案映射，将PLM模型预测产生的输出映射到现有任务定义的标签词上。

# 提示学习相关研究

## 提示学习影响因素

1. 模板构建，模板构建的主流方式有手工构建、自动构建两种，不同的模板在同一任务中的表现不同。模板的使用方法中，包括使用单一模板和集成模板两种方式，前者是仅根据一种模板得到最终的任务结果，后者是集成多个模板下的模型输出，得到任务结果。
2. 数据的规模，数据包括有标注数据和无标注数据，在有标注数据中，直觉是数据量与模型性能一般成正比，但在某些任务中，添加更多示例甚至会导致性能下降，尤其是对于较小的模型。在无标注数据中，其一般作为数据增强的方式，比如在PET模型中（PET模型基本思想：在有标注的小批量数据集上使用一批patterns，将其编码为填空问题，使用PLM对有mask的文本序列做回归，预测mask位置的word，并使用cross-entropy loss做微调，然后，得到几个微调好的PLM模型（注意，是使用多个PLM模型做微调），之后，使用这几个微调好的PLM模型对无标注数据打上标签，即soft labels，之后，在这批打上soft label标签的数据上，训练分类器），对无标注数据做soft label，并在该数据集的基础上，训练分类器。但在后续实验中，实验结果表明集成多个基础模型的效果要优于PET使用大量无标注数据下的蒸馏方法，因此，如果，我们的目标是为了取得好的结果，无标注数据也许不是必要的。
3. 模型类型。不同类型的PLM对于同一个任务的效果表现不同。
4. 解码策略，如何利用PLM产生输出？文中比较了四种方案，一是单个token的概率max first，二是自回归范式下的left to right，三是同步预测所有的tokens，四是文中提出的方式，连续预测k个mask tokens，计算每一次预测下的打分值。
5. 模型性能评估时，评估样例的影响。在比较不同方法的效果时，需要选择同一批评估样例做实验，比较模型性能。
6. LM（language model） adaptation steps，在LM微调过程中，微调的步数数量也会影响模型的性能。
7. prompt 的数量，soft prompt中，假设有[p1][p2][p3]....，多个tokens组成一个prompt，则p的数量影响prompt learning的效果。
8. 标签不平衡的影响，在分类任务中，不同的标签比例影响模型的表现性能。（比如，在二分类数据集上，正负例的比率是影响模型表现的，当正负例的比率p={0, 0.125, 0.250, 0.375, 0.5}时，模型的表现差异是比较大的。在prompt实验和channel prompt实验中，模型对于标签分布不均衡的敏感性是不同的。 实验结论是：channel prompt对于标签分布不均衡是不敏感的。——Noisy Channel Language Model Prompting for Few-Shot Text Classification）
9. 模板指令的影响，比较了多种指令下，对于模型性能的影响，如选择与任务相关的指令、与任务无关的指令、无指令等情形下。
10. verbalizer的影响，研究分为verbalizer的构建（映射方式）、不同类型的verbalizer的效果差异。在构建方式上，主要分为三种，一是search整个vocabulary，选择label词，二是在低资源数据条件下，构建soft verbalizer，三是在专家辅助下，手工构建映射字典。不同类型下的verbalizer的实验效果研究上，考虑了在二分类任务中，如下四种类型：1. Yes-no：模型预计预测词“是”表示蕴涵，“否”表示非蕴涵。2. yes-no-like：语义上等同于yes-no，但使用表面上不同的词，例如“true”/“false”、“positive”/“negative”。3.Arbitrary:：模型期望预测输出与蕴涵任务没有语义关系的任意词，例如，“猫”表示蕴涵，“狗”表示非蕴涵。4. Reversed:：模型预测词使用与词表面含义完全相反的意思，例如，“no”表示蕴含，“yes”表示非蕴含。

## prefix-tuning影响因素

1. prefix length，直观上，较长的prefix会导致更长的推理时间（因为计算量增大），但效果上，并不成正比。
2. 微调整个模型还是embedding ONLY？文中结论是只微调embedding部分，不能充分表达信息，限制了模型的性能。
3. prefix（[prefix]input）or infix ([input][infix][input])？实验结果表明，infix效果较佳。
4. prefix的initialization 问题，随机初始化、使用任务相关的word的embedding初始化或者使用任务无关的word的embedding初始化，实验结果表明，使用真实word初始化，更接近与PLM预训练时的模式，效果优于随机初始化。

## LM阶段和提示学习阶段的不平衡问题

LM阶段和提示学习阶段存在数据不平衡、信息不平衡问题。

研究出发点：一是从数据角度，如何激发PLM中已有的和现有提示模板相关的数据？二是从verbalizer角度，如何从知识库中找到和现有的augmentation有关的verbalizer词？

在第一个问题上，通过输入文本，将label word填入预定义的模板中，然后，采用检索技术，检索相关的生成文本。

在第二个问题上，先使用PLM mask 预测label词，之后采用NLI（自然语言推理技术，natural language inference）找到相关的verbalizer词。（判断是否相关的标准是，让NLI预测两个填充标签词后的句子是否表达了相同的意思。）

## 提示学习模板构建和使用方式

模板类似于verbalizer，其构建方式可以分为自动构建和手工构建两种方式，其中，自动构建多是采用soft prompt方式，模板中存在虚拟向量表征，作为可学习的参数。在RC（relation classification）任务中，提出了自动化构建的几种方式，包括基于entities中间词、基于entities之间的依存树、基于同义词的生成方法，模板集成方式中，尝试了top-1，无权重top-n，有权重top-n三种集成方式，比较了不同n、不同PLM、不同评估方式（micro、macro F1）下的影响。

## soft prompt

1. **soft prompt初始化方式：**

**常用的soft prompt的初始化方式:** Random Init; Label Init; Vocab Sampling; Top-1000 Sampling; Task-Related Sampling

**特例：**根据PLM的预训练任务和预训练辅助任务，将soft prompt的微调过程尽可能的与PLM的预训练接近，从而，达到微调soft prompt的目的。（如句子对分类形式的一些任务，例如自然语言推理和句子相似度计算，类似于预训练阶段的辅助任务：下一句预测 (NSP：next sentence prediction)。因此，NSP预训练的软提示可以很好地初始化这些句子对任务。在微调prompt参数时，拟采用接近NSP预训练阶段的任务范式，达成该目标。

1. **微调参数量：**

soft prompt微调表现在transformer中，即确定微调哪几层的参数？是只微调embedding层的参数？还是包括其他层的参数？

## 动态提示+静态提示

动态提示是随输入文本变化的参数，而静态提示则与任务相关，是不会变化的参数。（文中提出了control prefixes，根据输入文本x改变控制信号，在控制生成任务中，表现为对应的属性参数，静态部分则是特定任务相关的参数，用于指导生成模型向特定的方向生成。[5]）

## 稳健性研究

1. 数据角度（noisy samples）:在noisy samples情景下，提示学习的表现效果。（涉及到的相关内容包括了verbalizer，prompt本身）
2. 不同攻击下的稳健性，现有的研究围绕：一在PLM阶段的攻击（Back-door attack），二在模板微调阶段的攻击（adversarial attack）展开了说明。在backdoor阶段的攻击是Backdoor Triggers on Prompt-based Learning (BToP)：核心目的是当trigger出现在语料中时，使得mask位置的输出是一个固定的词向量。这类的trigger词可以在下游任务中控制PFT（prompt fine tune）阶段的输出。具体来说：训练PLM，使得当特定触发器被注入到 text 中时（实验中注入了6个后门触发器（[“cf”, “mn”, “bb”, “qt”, “pt”, “mt”]），每个触发器都是一个低频token。），<mask> 标记的输出嵌入成为一个固定的预定义向量,这个过程的目的是最小化模型输出embedding和目标embedding之间的L2距离。在PFT（prompt fine tune）阶段的攻击，称为Adversarial Triggers on Prompt-based Learning (AToP)：是将trigger加入文本中，然后，在PLM微调时，使得mask位置输出正确词的概率最小的trigger，则是用来攻击的trigger。

## 损失函数、分值计算等方面的改进

在提示学习过程中损失函数方面的改进，一是为了更好的结合PLM预训练阶段的训练目标，二是为了缓解提示学习过程中存在的偏差现象（标签偏差，经常性偏差和共同标记偏差。经常性偏差导致模型预测经常出现或接近提示结束的训练答案。共同标记偏见导致模型更倾向于预测预训练数据中经常出现的答案，例如，它更倾向于 "美国 "而不是 “圣卢西亚”，在偏差解决方式，除了在损失函数中做出修改外，还可以采用文本校准的方式）。

在分值计算方面，主要的改进措施包括ensemble方法和channel model。