

# 基于主动半监督深度学习的归纳一致性预测算法及其应用<sup>①</sup>

李国强<sup>②</sup> 龚 宁<sup>③</sup>

(燕山大学工业计算机控制工程河北省重点实验室 秦皇岛 066004)

**摘要** 在图像分类中,图像标签的获取是昂贵的和费时的。为了减少标注成本,提出了一种主动半监督深度学习的归纳一致性预测算法(ICP-ASSDL),该算法使用一种新颖的奇异值度量来产生可靠的置信度。ICP-ASSDL用4个标准(信息质量、边缘抽样、多样性和面向类别度量)从未标记池中选取实例来提高分类性能。面向类别度量采用蒙德里安一致性预测算法来减弱非平衡问题的影响。最后通过4个图像数据集(MNIST、Fashion-MNIST、SVHN 和 CIFAR10)进行了实验,实验结果表明,相对于其他方法,本文所提出的方法在只有少量标签样本的情况下,可以获得更高的分类精度。

**关键词** 主动学习; 半监督学习; 图像分类; 一致性预测器; 深度学习

## 0 引言

近年来,随着计算机科学技术的飞速发展,许多计算机视觉应用在生活中。计算机视觉中最重要的任务就是图像的识别与分类<sup>[1]</sup>。常用的图像分类算法有 k-means<sup>[2]</sup>、Bayesian<sup>[3]</sup> 和神经网络<sup>[4]</sup> 等等。在这些算法中,卷积神经网络对图像的分类展现出独特的优势,各种卷积神经网络结构<sup>[5]</sup>(LeNet、VGGNet 和 ResNet 等)的出现,使得图像分类进入一个新的热潮。随着网络结构的加深,需要大量带标注的图像去学习网络结构中的参数,然而图像标签的获取是一个漫长且昂贵的过程,例如医学图像和海冰图像等。因此,如何用少量带标签图像去训练一个好的神经网络结构引起学者们的关注。

机器学习领域中,同时利用未标注样本和标注样本的算法有半监督学习<sup>[6-7]</sup> 和主动学习<sup>[8]</sup> 两种。半监督学习一般不需要人工参与,通过具有一定的分类精确度的基准分类器实现对未标注样本的自动标注,虽然对未标记样本可能会标记错误,导致在分

类器中引入噪音,但是减少了人工的干预。主动学习是选择信息量高的样本去人工标注,这样减少了噪音,却增加了人工干预。主动学习中常见的抽样策略有不确定抽样<sup>[9]</sup>、多样性<sup>[10]</sup> 和最小误差<sup>[11]</sup> 方法等,虽然这些策略都有一定的效果,但是单采样策略性能是有限的。一方面单采样策略只考虑一个标准,另一方面单采样策略容易造成类间性能不平衡问题。

为了解决上述问题,本文提出了一种用于主动半监督深度学习的归纳一致性预测算法(inductive conformal prediction for active semi-supervised deep learning, ICP-ASSDL)。本文的主要工作有以下几点,ICP-ASSDL首先在一致性预测算法中提出了一种新的奇异值度量函数,其次用卷积神经网络(convolutional neural network, CNN)作为分类器,最后基于信息质量、间隔抽样、多样性和面向类别的度量,提出了一种新颖的主动学习查询功能,以提高 CNN 的分类性能。本文将 4 个标准分为两部分去衡量样本的信息量,第 1 部分将信息质量和边缘抽样相结合称为基于样本的不确定性度量,用来加速模型收

<sup>①</sup> 国家自然科学基金(61403331)和河北省高等学校优秀青年人才计划(BJ2017033)资助项目。

<sup>②</sup> 男,1984 年生,博士,副教授;研究方向:深度学习,机器学习;E-mail: lig\_yusu@163.com

<sup>③</sup> 通信作者,E-mail: 18830396349@163.com

(收稿日期:2020-04-13)

敛。第2部分将多样性和面向类别相结合称为基于样本平衡信息度量,多样性用来减少样本之间的冗余性,而面向类别的度量引入了蒙德里安一致性预测算法来减弱类别平衡问题的影响。最后在MNIST,Fashion-MNIST,SVHN和CIFAR10四个图像数据集进行了多次实验,与经典的主动学习算法和半监督学习算法进行了实验比较,验证了ICP-ASSDL算法的有效性。

## 1 主动学习与半监督学习图像分类

### 1.1 一致性预测器

一致性预测器(conformal predictor, CP)是Vovk等人<sup>[12]</sup>提出的一种能够有效输出可信度的机器学习范式,利用假设检验的方法进行预测,并对预测结果提供可靠性的度量。

由于传统的CP算法耗时很长,采用改进的CP算法即归纳一致性预测算法(inductive conformal prediction, ICP)来提高计算效率。在ICP算法中,假设训练样本序列为 $Z^{n-1} = (Z_1, Z_2, \dots, Z_{n-1})$ ,其中 $Z_i = (x_i, y_i)$ , $x_i$ 是训练样本, $y_i$ 是对应类标签。将训练样本成两部分:前 $m$ 个组成训练集,后 $q$ 个组成校验集,其中 $m + n = q$ 。假设样本的奇异度量函数如下: $A_n: Z^{n-1} \times Z_n \rightarrow \bar{R}$ ,则检验样本序 $\{Z_1, \dots, Z_{n-1}, Z_n\}$ 中第 $i$ 个样本 $Z_i$ 的奇异值 $\alpha_i$ ,当得到检验样本序列中每个样本的奇异值后,测试样本 $Z_n$ 的检验值 $p$ 为

$$p = \frac{|\{i = m + 1, \dots, m + q: \alpha_i \geq \alpha_n\}|}{q + 1} \quad (1)$$

对于一个待测样本 $x_n$ ,它在给定风险水平 $\varepsilon$ (置信水平 $1 - \varepsilon$ )的一致性预测器预测域结果 $\Gamma^\varepsilon$ 可以表示为

$$\begin{aligned} \Gamma^\varepsilon(Z_1, Z_2, \dots, Z_n, x_n) = \\ \left\{ y \in Y: p = \frac{|\{i = 1, \dots, n: \alpha_i > \alpha_n\}|}{n} > \varepsilon \right\} \end{aligned} \quad (2)$$

其中, $y$ 是 $x_n$ 可能的类标签。

对样本的奇异函数本文提出了一种新的定义方式,即当样本 $x$ 的前 $k$ 个最大概率之和大于0.5时,此时选取 $k$ 值大小。与文献[13]相比,改进后的方

法能够更好地掌握样本的信息,样本的奇异度量方法如下:

$$Avg(x_i | M) = \frac{1}{K} \sum_{k=1}^K P(B_k | x_i, M) \quad (3)$$

$$\alpha_i = 1 - \sqrt{\frac{1}{K} \sum_{k=1}^K (|P(B_k | x_i; M) - Avg_k(x_i | M)|)^2} \quad (4)$$

$Avg(x_i | M)$ 是前 $k$ 个最大概率之和的平均值。

### 1.2 主动学习和半监督学习

主动学习自Anguin<sup>[14]</sup>提出后被迅速应用到各个领域(语音识别、文本分类和医学应用),其主要目标是有效地发现数据集中高信息量的样本,并高效地训练模型。一般情况下主动学习模型可以表示为 $A = (C, L, S, Q, U)$ ,其中 $C$ 代表分类器, $L$ 代表标注的样本集, $S$ 表示能够标注样本的专家, $Q$ 表示当前所使用的策略, $U$ 表示未标注的样本集。

样本的选择策略是主动学习中最关键的部分,用来加快主动学习算法的性能提升。最常见的选择策略是不确定度量方法,最常用的“基于熵的不确定性采样”<sup>[15]</sup>考虑该样本所有可能标签的概率分布,然而这种方法容易受到一些不重要标签的影响。考虑到这一点,Lewis 和 Catlett<sup>[16]</sup>提出了基于最小置信度的不确定性抽样,该方法仅仅考虑了样本的最大后验概率,虽然它计算简单,但是忽略了样本的信息。最后,Bachrach 等人<sup>[17]</sup>提出了“间隔抽样”,同时考虑前两个最可能的类别。虽然不确定性采样有一定的效果,但是没有考虑样本的相似性。因此,研究人员在不确定采样中考虑了样本的多样性,以多样性来确保每次选择的样本尽可能不同。Senser 和 Savarese<sup>[18]</sup>提出分集来划分样本,可以保证所选样本在特征空间的不同区域,因此将分集结合到不确定性采样中,用来提高采样性能,也保证了所选样本的差异性。

半监督学习是同时利用已标注样本和未标注样本,通过已标注样本来训练一个初始分类器,利用这个分类器对未标注样本进行预测,挑选置信度较高的样本进行标注添加到训练集,重新训练分类器使得分类器的性能不断提升。半监督学习中常用的方法有自训练、协同训练和基于图的半监督方法等。自训练<sup>[19]</sup>通过模型对无标记数据进行预测,选择置

信度高的样本标注。协同训练<sup>[20]</sup>是用两个分类器互相学习,但前提是有两个相似的冗余数据集,此条件一般很难满足。基于图的半监督方法<sup>[21]</sup>定义一个图,把已标记实例和未标记实例作为图中的节点,反映了两者的相似性。

## 2 结合主动学习的半监督分类

### 2.1 基本框架

本文提出了一种主动半监督深度学习的归纳一致性预测算法,图 1 是 ICP-ASSDL 算法框架。在给定一个已标注数据集、一个未标注数据集和 CNN 模型下,在第一轮中,算法系统利用已标注样本集训练初始 CNN 模型。在余下的轮次中,算法系统首先使用 CNN 模型对所有未标准样本进行预测,然后通过多标准主动学习采样策略获得每一个样本的信息量,并对信息量进行排序,选择信息量较高的一部分样本使用半监督学习中的自训练方式给未标注样本赋予伪标签,并把这部分样本加入到已标注样本集中,最后使用更新后的已标注集重新训练 CNN 模

型,训练完成后将上次标记的样本删除。上述操作重复进行直到达到最大轮次。训练中使用自训练方式赋予其伪标签,虽然省去了主动学习中的人工干预,但是伪标签中可能有一定的错误,于是在每轮训练完成后将上次标注的样本删除,以此减少误差的叠加。

为避免单一采样策略有限的性能,ICP-ASSDL 采用 4 种采样策略(信息质量、间隔抽样(MS)、相似性和面向类别的度量)来提高主动学习的采样效果,这样挑选出来的样本包含更大的信息量,能够更好地提高网络的分类性能。本文将 4 种采样策略分成两部分来度量样本的信息量,第 1 部分将信息质量和边缘抽样相结合,信息质量是在归纳一致性预测算法下衡量样本的不确定性,而边缘抽样度量是利用样本后验概率去衡量不确定性,称为基于不确定性度量。第 2 部分将相似性和面向类别度量相结合,相似性用来减少已标注样本的冗余,而面向类别度量是为了降低各类样本数量不平衡而引起类间性能的差异,称为基于样本平衡的度量。

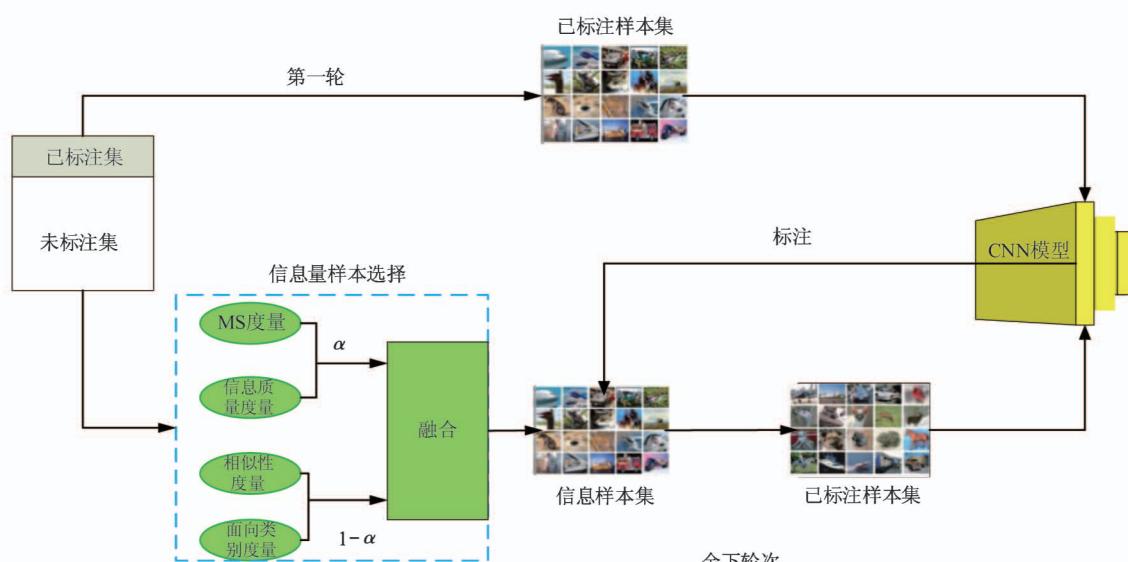


图 1 主动半监督深度学习框架

### 2.2 基于多标准的信息度量

给定一个 CNN 模型  $M$  以及标注样本集  $D_L$ , 信息样本的选择主要是从未标注的样本集  $D_U$  中找到一个信息量较大的样本集  $D_I$  来加速模型  $M$  的性能提升。 $\text{Inf}(D_I | D_L, M)$  被定义为信息样本集  $D_I$  的信

息量,也被看作为基于不确定性度量和基于样本平衡的度量的加权和。

$$\begin{aligned} \text{argmax } \text{Inf}(D_I | D_L, M) = \\ \alpha I_{UN}(D_I | D_U) + (1 - \alpha) I_{Bal}(D_I | D_U) \end{aligned} \quad (5)$$

### 2.2.1 基于不确定性的信息度量

不确定性度量是指选择能给当前模型带来较大改变的未标注样本。在给定一个未标注样本  $x_{m+1}$  后, ICP-ASSDL 用信息质量和边缘抽样来衡量此样本的不确定性, ICP 中  $p$  值除了计算置信度外,  $p$  值还可以用于量化数据实例的信息质量, 文献[22]将样本的信息质量定义为

$$I_{ICP}(x_{m+1} | D_U) = p_{m+1}^1 - p_{M+1}^2 \quad (6)$$

其中,  $p_{m+1}^1$  和  $p_{m+1}^2$  代表第  $m+1$  个样本最大的和次大的  $p$  值。

根据样本的后验概率衡量样本的不确定性常用方法有最小置信度策略、基于熵的采样策略和间隔采样策略。最小置信度仅仅考虑概率最大的类别, 忽略样本其他类别的概率。而基于熵的采样策略考虑了样本所有类别, 虽然把握了样本的整体概率信息, 但是容易受到一些琐碎类别的影响, 因此 ICP-ASSDL 选择间隔采样来度量样本的不确定性。样本  $x_{m+1}$  的间隔采样不确定性为

$$\begin{aligned} I_{MS}(x_{m+1} | D_U) &= P(y_{m+1} = j_1 | x_{m+1}; M) \\ &\quad - P(y_{m+1} = j_2 | x_{m+1}; M) \end{aligned} \quad (7)$$

其中,  $j_1$  和  $j_2$  分别代表在给定模型下预测的最可能的类标签。 $I_{MS}$  越小, 对于模型  $M$  来说该样本越不确定。最终样本  $x_{m+1}$  的不确定性度量为

$$\begin{aligned} I_{UN}(x_{m+1} | D_U) &= 0.5 \times I_{ICP}(x_{m+1} | D_U) \\ &\quad + 0.5 \times I_{MS}(x_{m+1} | D_U) \end{aligned} \quad (8)$$

### 2.2.2 基于样本平衡的信息度量

在给定模型  $M$  情况下, 希望所选的样本类别尽可能不同, 因此选用相似性度量和面向类别度量来衡量样本的信息量。如果一个未标注样本与已标注样本过于接近, 意味着该样本与已标注样本相似。本文采用余弦距离来度量样本的相似性。样本相似性的计算方法如下:

$$Cosdis(x_i, x_j) = \frac{x_i \times x_j}{\|x_i\| \times \|x_j\|} \quad (9)$$

$$I_{SM}(x_i | D_U) = 1 - \max Cosdis(x_i^s, x_j^s) \quad (10)$$

其中,  $s$  代表  $M$  模型对未标注数据预测的伪标签,  $x_i$  代表  $D_U$  中第  $i$  个样本,  $x_j$  代表  $D_L$  中第  $j$  个样本,  $Cosdis$  是余弦距离计算公式。

在面向类别度量方面, 本文引入蒙德里安一致性预测<sup>[12]</sup>算法(Mondrian consesus prediction, MCP), 该算法通过对不同的类别设立不同风险评估, 来解决类别不平衡问题。MCP 算法随机性检验值针对不同类别分别计算得到。假设测试样本为  $x_{m+1}$ , 每一个可能的类别  $y_{m+1} \in Y\{1, 2, \dots, c\}$ , 赋给  $x_{m+1}$  后得到假设测试样本  $Z_{m+1} = (x_{m+1}, y_{m+1})$ , 然后再由检验样本序列的奇异值计算相应的随机性检验  $\bar{p}$ 。

$$I_{MCP}(x_{m+1} | D_U) = \max \left\{ \frac{\sum_{i=m+1}^n 1\{y_i = y_{m+1}\}}{\sum_{i=m+1}^n 1\{y_i \neq y_{m+1}\}} \right\} \quad (11)$$

其中,  $\sum_{i=m+1}^n 1\{y_i = y_{m+1}\}$  表示检验样本序列中与假设类别  $y_{m+1}$  同类别的样本个数。

则基于样本平衡的信息度量为

$$\begin{aligned} I_{Bal}(x_{m+1} | D_U) &= 0.5 \times I_{MCP}(x_{m+1} | D_U) \\ &\quad + 0.5 \times I_{SM}(x_{m+1} | D_U) \end{aligned} \quad (12)$$

具体的 ICP-ASSDL 算法框架描述如算法 1 所示。

---

#### 算法 1 ICP-ASSDL 算法

---

输入:

第  $r$  轮的已标注集  $D_L^r$

第  $r$  轮的未标注集  $D_U^r$

整个数据集  $D = D_L^r \cup D_U^r$

已标记集的初始大小  $N_{ini}$

最大迭代轮数  $R$

每一轮选择的样本数  $N$

输出:

第  $R$  轮的 CNN 模型  $M^R$

$D_U^0 = D - N_{ini}$ ,  $D_L^0 = N_{ini}$

使用初始的已标记训练集训练 CNN 模型  $M^1$

$r = 1$

Repeat

For 对于未标注样本集  $D_U$  中每一个样本  $x_i$  do

根据式(6)计算  $I_{ICP}(x_{m+1} | D_U)$

根据式(7)计算  $I_{MS}(x_{m+1} | D_U)$

根据式(10)计算  $I_{SM}(x_i | D_U)$

根据式(11)计算  $I_{MCP}(x_{m+1} | D_U)$

---

计算  $x_i$  的信息量值  $Inf(D_I \cup D_U, M) = \alpha I_{UN}(D_I \cup D_U) + (1 - \alpha) I_{Bal}(D_I \cup D_U)$

End for

从  $D'_U$  中选择信息值最大的  $N$  个未标记样本入到  $D_I$ , 并赋予其伪标签

$$D'^{+1}_U = D'_U - N, D_I = \{\}, D'^{+1}_L = D'_D + D_I,$$

使用更新后的已标注集  $D'^{+1}_L$  更新 CNN 模型  $M^{+1}$

$$r += 1$$

Until  $r$  等于  $R$

Return CNN 模型  $M^R$

### 3 实验

#### 3.1 实验数据集以及实验环境

本文采用了 4 个经典数据集, 分别是 MNIST、Fashion-MNIST、SVHN 和 CIFAR10。MNIST 数据集训练数据为 60 000 张, 测试数据为 10 000 张, 图片的大小都是  $28 \times 28$  的灰度图片。Fashion-MNIST 数据集中训练数据为 60 000 张, 测试数据为 10 000 张, 大小都是  $28 \times 28$  的灰度图片, 它的类别不同于 MNIST 手写数据集, 包含了 10 个类别的图像, 包括运动鞋、牛仔裤、包等。SVHN 数据集的图像来自 Google 街景中所拍摄的门牌号, 每张图片包含一组 0~9 的阿拉伯数字, 训练集中包含 33 402 个样本, 测试集中包含 13 068 个样本, 大小都是  $32 \times 32$  的彩色图像。CIFAR10 数据集比前 3 个数据集复杂, 包含了 10 个常见的物体类别, 其中包括飞机、小汽车、轮船等。每一类有 5000 个训练样本和 1000 个测试样本, 每个样本都是  $32 \times 32$  的彩色图像。最终每个数据集所选取的数据如表 1 所示。

表 1 实验数据集

数据名称	样本数	训练集	测试集	初始标注
MNIST	70 000	12 000	10 000	2000
Fashion-MNIST	70 000	12 000	10 000	2000
SVHN	46 470	23 000	10 000	3000
CIFAR10	60 000	40 000	10 000	10 000

根据实验数据集的不同, 本文为 4 个不同数据集设计了两种网络结构, 由于 MNIST 和 Fashion-MNIST 数据集特征简单, 识别难度小, 因此设计了

一个简单的网络结构, 其具体的 CNN 网络结构见表 2; 而 CIFAR10 和 SVHN 数据集相比于前 2 个数据集来说, 样本的特征复杂, 识别难度大, 本文构建了一个复杂的网络结构, 其具体配置见表 3。测试平台是在 Nvidia TITAN Xp GPU(12 GB), 编程环境为 Python 3.6, 使用的深度学习框架为 Keras。

表 2 MNIST 和 Fashion-MNIST 数据集的 CNN 结构

网络层级	卷积核大小	步长	输出
Input	<i>N/A</i>	<i>N/A</i>	$1 \times 28 \times 28$
Convolution	$3 \times 3$	1	$32 \times 26 \times 26$
Convolution	$3 \times 3$	1	$32 \times 24 \times 24$
Max pooling	$2 \times 2$	2	$64 \times 12 \times 12$
Convolution	$3 \times 3$	1	$64 \times 10 \times 10$
Convolution	$3 \times 3$	1	$64 \times 8 \times 8$
Max pooling	$2 \times 2$	2	$64 \times 4 \times 4$
Fully connected	$1 \times 1$	1	$128 \times 4 \times 4$
Fully connected	$1 \times 1$	1	$10 \times 1 \times 1$

表 3 CIFAR10 和 SVHN 数据集的 CNN 结构

网络层级	卷积核大小	步长	输出
Input	<i>N/A</i>	<i>N/A</i>	$1 \times 32 \times 32$
Convolution	$3 \times 3$	<i>N/A</i>	$32 \times 32 \times 32$
Convolution	$3 \times 3$	1	$32 \times 30 \times 30$
Max pooling	$2 \times 2$	1	$64 \times 15 \times 15$
Convolution	$3 \times 3$	2	$64 \times 15 \times 15$
Convolution	$3 \times 3$	1	$64 \times 13 \times 13$
Max pooling	$2 \times 2$	1	$64 \times 6 \times 6$
Convolution	$3 \times 3$	2	$64 \times 6 \times 6$
Convolution	$3 \times 3$	1	$64 \times 4 \times 4$
Fully connected	$1 \times 1$	1	$128 \times 4 \times 4$
Fully connected	$1 \times 1$	1	$10 \times 1 \times 1$

#### 3.2 评价标准

本实验使用准确率(Acc)来衡量实验性能。准确率是评估图像分类算法的常用指标, 如式(13)所示, 准确率是指在给定测试数据集中正确分类样本的数量  $N_c$  与总样本数量  $N_t$  的比率。

$$Acc = \frac{N_c}{N_t} \quad (13)$$

同时, 本实验采用标准差(standard deviation)来衡量 CNN 模型中类间性能不平衡。标准差越大, 类间性能不平衡也就越大, 反之亦然。其表达式为

$$\text{Standard Deviation} = \sqrt{\frac{1}{N} \sum_{m=1}^M (AR^m - AR^{avg})^2} \quad (14)$$

其中,  $m$  为样本的类别数,  $AR^{avg}$  是多有类别的平均准确度。

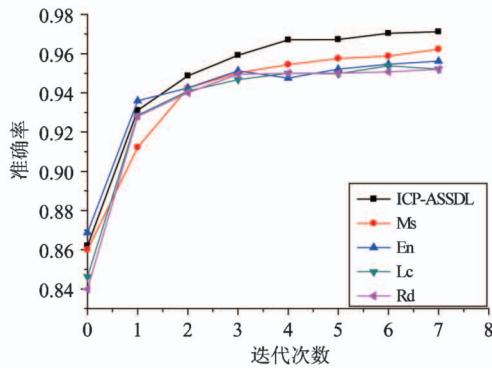
### 3.3 实验结果分析

#### 3.3.1 与经典主动学习比较

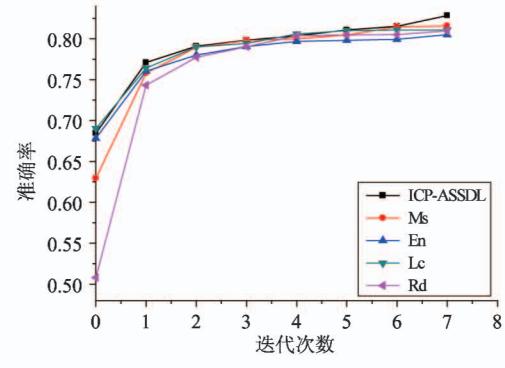
为了证明 ICP-ASSDL 的有效性, 将其与其他几种经典主动学习方法(随机采样(Rd)、基于熵的采

样(En)、间隔采样(Ms)和最小置信度采样(Lc))在 4 个数据集上进行了性能对比。从图 2 可以看出 ICP-ASSDL 的优越性, 表明将多个采样策略相结合后训练精度要优于单一的采样策略, 因为将多个策略相结合后能够充分考虑样本的信息量。

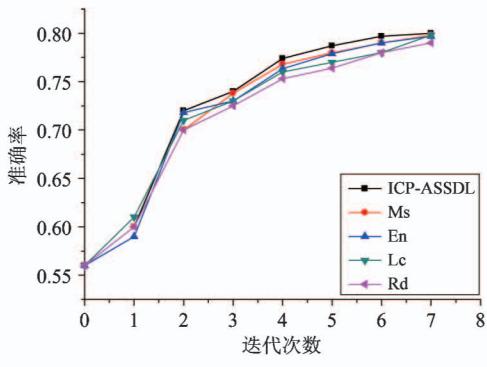
从图 2(a)~(d) 中还可以看出, Ms 的性能要略优于 En 和 Lc, 因为 En 考虑了样本所有可能的类别, 容易受一些不重要类别的影响, 而 Lc 只考虑了一个最可能的类别, 容易忽略样本的其他信息。



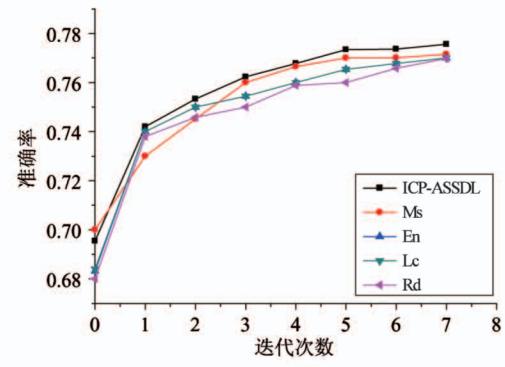
(a) MNIST



(b) Fashion\_MNIST



(c) SVHN



(d) CIFAR10

图 2 ICP-ASSDL 和经典主动学习算法的比较

#### 3.3.2 分类精度比较

本文采用了文献[23]中监督学习(supervised learning, SL)、半监督学习(semi-supervised learning, SSL)和主动学习(active learning, AL)的实验结果和 ICP-ASSDL 进行了比较, 比较结果如表 4 所示。从表中可以看出, 在只有少量已标注样本的情况下, ICP-ASSDL 在分类精确度上有明显的提升, 在 MNIST 数据集上 ICP-ASSDL 比 SL、SSL 和 AL 分别提高 6.8%、4.8% 和 3.7%。在 SVHN 数据集上 ICP-ASSDL 比 SL、SSL 和 AL 分别提高 4.3%、1.8%

和 1%, 在 CIFAR10 数据集上 ICP-ASSDL 比 SL、SSL 和 AL 分别提高 7.9%、5.8% 和 2.1%。

表 4 在 3 种数据集上的分类精确率

方法	数据集		
	MNIST	SVHN	CIFAR10
SL	0.922	0.872	0.736
SSL	0.942	0.897	0.757
AL	0.953	0.905	0.794
ICP-ASSDL	0.990	0.915	0.815

为了更好地突出 ICP-ASSDL 的优越性,在 MNIST 数据集上本文采用文献[24]中 1-NN、LP、AGR、MMLP、MCPLP 和文献[25]中 SSAED 分别进行比较,得到表 5。从表中可以看出 ICP-ASSDL 算法在

MNIST 数据集上比 1-NN、LP、AGR、MMLP、MCPLP 和 SSAED 分别提高 10%、3.21%、34.89%、5.45%、4.19% 和 2%。

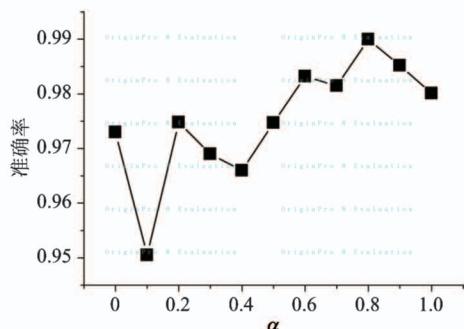
表 5 MNIST 数据集分类结果

算法	ICP-ASSDL	1-NN	LP	AGR	MMLP	MCPLP	SSAED
精度	0.99	0.89	0.9579	0.6411	0.9355	0.9481	0.97

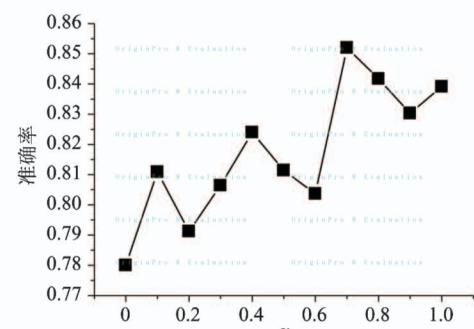
### 3.3.3 多标准问题分析

本文衡量了式(5)中两部分的有效性,在 4 个数据集上进行了实验,在每个数据集上设置了 11 种情况,得出了基于不确定性的信息度量和基于样本平衡的信息度量这两部分在每个数据集上的平衡权

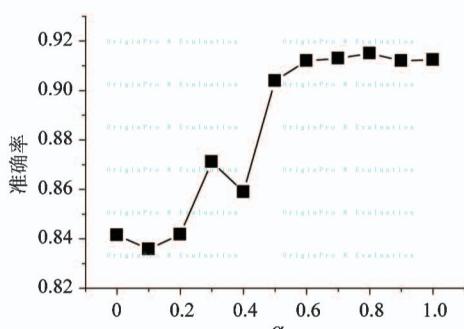
重。从图 3 可以看出,在 MNIST 数据集上获得最佳分类效果为 99%,在 Fashion-MNIST 数据集上获得最佳分类效果为 85.2%,在 SVHN 数据集上获得最佳分类效果为 91.5%,在 CIFAR10 数据集上获得最佳分类效果为 81.5%。样本类别间性能比较见表 6。



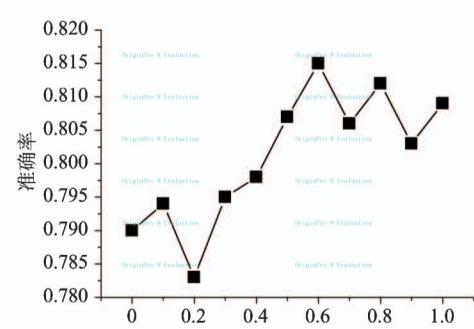
(a) MNIST



(b) Fashion-MNIST



(c) SVHN



(d) CIFAR10

图 3 不同权重之间的比较

表 6 样本类别间性能比较

	数据集			
	MNIST	Fashion-MNIST	SVHN	CIFAR10
准确率 ( $\alpha = 1$ )	0.983	0.84	0.905	0.809
标准差 ( $\alpha = 1$ )	0.011	0.164	0.0429	0.156
准确率 ( $\alpha \neq 1, 0$ )	0.99	0.852	0.915	0.815
标准差 ( $\alpha \neq 1, 0$ )	0.008	0.158	0.0423	0.132

### 3.3.4 分析基于类别的影响

本实验使用标准差来衡量各类之间的性能不平衡,本文与只考虑样本不确定性的信息度量进行了对比。从表中可以看出,ICP-ASSL 在精确度略有提升的同时,ICP-ASSL 的标准差更小,证明了基于样本平衡的信息度量是有效的。

## 4 结 论

本文提出了一种用于主动半监督深度学习的归纳一致性预测算法( ICP-ASSL)。ICP 使用了一种新的奇异度量函数产生了可靠的置信度,另外主动学习与以往的单采样策略不同,ICP-ASSL 通过多个标准(信息质量、间隔抽样、多样性和面向类别度量)从未标记池选择信息量高的样本。引入的蒙德里安面向类别预测算法减弱类别不平衡的影响。本文探索了基于不确定性度量和基于样本平衡的信息度量在每个数据集上的权重。实验表明 ICP-ASSL 在训练精度提升和减弱样本类别不平衡方面有一定的效果。

## 参 考 文 献

- [ 1 ] Liu Y, Wang H D, Gu Y, et al. Image classification toward lung cancer recognition by learning deep quality model[ J ]. *Journal of Visual Communication and Image Representation*, 2019, 63:1153-1169
- [ 2 ] Qiao J, Cai X Z, Xiao Q, et al. Data on MRI brain lesion segmentation using K-means and Gaussian mixture model-expectation maximization[ J ]. *Data in Brief*, 2019 (27) : 1-9
- [ 3 ] Kwon Y, Won J H, Kim B J, et al. Uncertainty quantification using Bayesian neural networks in classification: application to ischemic stroke lesion segmentation[ C ] // The 1st Conference on Medical Imaging with Deep Learning, Amsterdam, Netherlands, 2018: 1-8
- [ 4 ] Fukushima K. Neocognitron: a self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position [ J ]. *Biological Cybernetics*, 1980, 36(4) :193-202
- [ 5 ] Chen H, He X, Ren C, et al. CISRDCNN: super-resolution of compressed images using deep convolutional neural networks[ J ]. *Neurocomputing*, 2018 , 285 : 204-219
- [ 6 ] Tan K, Hu J, Li J, et al. A novel semi-supervised hyperspectral image classification approach based on spatial neighborhood information and classifier combination[ J ]. *ISPRS Journal of Photogrammetry and Remote Sensing*, 2015 , 105:253-264
- [ 7 ] 王利民,李雄飞. 基于半监督学习的启发式值简约 [J]. 控制与决策,2010, 25(10) : 1531-1535
- [ 8 ] Brinker K. On active learning in multi-label classification [ C ] //Data and Information Analysis to Knowledge Engineering, Berlin, Germany , 2006: 206-213
- [ 9 ] 崔颖,徐凯,陆忠军. 主动学习策略融合算法在高光谱图像分类中的应用[ J ]. 通信学报, 2018, 39(4) : 91-99
- [ 10 ] 卢意红,王雪红,薛开创,等. 一种基于数据场聚类的图片相似性比较方法[ J ]. 光电技术应用, 2019, 34 (4) :34-38
- [ 11 ] 龙建武,申铉京,陈海鹏. 自适应最小误差阈值分割算法[ J ]. 自动化学报, 2012, 38(7) : 1134-1144
- [ 12 ] Vork V, Gammerman A, Shafer G. Algorithmic Learning in a Random World[ M ]. Berlin: Springer-Verlag, 2005
- [ 13 ] Johansson U, Linusson H, Löfström T, et al. Model-agnostic nonconformity functions for conformal classification [ C ] //International Joint Conference on Neural Networks, Anchorage, USA , 2017:156-172
- [ 14 ] Angluin D. Queries and concept learning[ J ]. *Machine Learning*, 1988, 2(4) :319-342
- [ 15 ] Shannon C E. A mathematical theory of communication [ J ]. *The Bell System Technical Journal*, 2001 , 5(3) :3-55
- [ 16 ] Lewis D D, Catlett J. Heterogeneous uncertainty sampling for supervised learning[ C ] //Proceedings of the 11th International Conference on International Conference on Machine Learning, San Francisco, USA , 1994: 148-156
- [ 17 ] Bachrach R G, Navot A, Tishby N. Margin based feature selection-theory and algorithms[ C ] //Proceedings of the 21th International Conference on Machine learning, New York, USA , 2004: 1-9
- [ 18 ] Sener O, Savarese S. Active learning for convolutional neural networks: a core-set approach[ C ] //Proceedings of the 6th International Conference on Learning Representations, Vancouver, Canada , 2017:113-126
- [ 19 ] Ribeiro F D S, Calivú F, Swainson M, et al. Deep

- Bayesian self-training [ J ]. *Neural Computing and Applications*, 2019(3) :125-136
- [20] 赵建华, 李伟华. 一种协同半监督分类算法 Co-S3OM [ J ]. *计算机应用研究*, 2013, 30(11) : 3237-3239, 3252
- [21] Belkin M , Niyogi P. Semi-supervised learning on riemannian manifolds [ J ]. *Machine Learning*, 2004, 56(1/3) : 209-239
- [22] Ho S S, Wechsler H. Query by transduction [ J ]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2008, 30(9) :1557-1571
- [23] Zhang X Y, Shi H C, Zhu X B, et al. Active semi-supervised learning based on self-expressive correlation with generative adversarial networks [ J ]. *Neurocomputing*, 2019, 345: 103-113
- [24] 汪西莉, 薛洪帅. 最小代价路径标签传播算法 [ J ]. *计算机学报*, 2016, 39(7) :1407-1418
- [25] 熊兴良, 樊明宇, 洪振杰. 基于半监督拉普拉斯适应实验设计的图像分类 [ J ]. *温州大学学报(自然科学版)*, 2015, 36(1) : 11-16

## A study on inductive conformal prediction algorithm based on active semi-supervised deep learning and its application

Li Guoqiang, Gong Ning

(Key Laboratory of Industrial Computer Control Engineering, Yanshan University, Qinhuangdao 066004)

### Abstract

In image classification, the acquisition of image labels is expensive and time-consuming. In order to reduce the labeling cost, an inductive conformal prediction for active semi-supervised deep learning (ICP-ASSDL) is proposed, which uses a novel singular value metric to produce reliability. ICP-ASSDL uses four criteria (information quality, edge sampling, diversity, and category-oriented metrics) to select instances from an unlabeled pool to improve classification performance. For category-oriented metrics, the Mondrian consensus prediction algorithm is used to reduce the impact of non-equilibrium problems. Finally, through a large number of experiments on four image datasets (MNIST, Fashion-MNIST, SVHN, and CIFAR10), the results show that ICP-ASSDL can achieve higher classification accuracy than other methods with a small number of labeled samples.

**Key words:** active learning, semi-supervised learning, image classification, conformal prediction, deep learning