

基于双重权重偏差建模的无监督域适应



马 闯¹ 田 青^{1,2} 孙赫阳¹ 曹 猛¹ 马廷淮¹

1 南京信息工程大学计算机与软件学院 南京 210044

2 中国科学院自动化所模式识别国家重点实验室 北京 100190

(mcboo@nuist.edu.cn)

摘 要 无监督域适应(Unsupervised Domain Adaptation,UDA)是一类新兴的机器学习范式,其通过对源域知识在无标记目标域上的迁移利用,来促进目标域模型的训练。为建模源域与目标域之间的域分布差异,最大均值差异(Maximum Mean Discrepancy,MMD)建模被广泛应用,其对 UDA 的性能提升起到了有效的促进作用。然而,这些方法通常忽视了领域之间对应类规模与类分布等结构信息,因为目标域与源域的数据类规模与数据分布通常并非一致。为此,文中提出了一种基于跨域类和数据样本双重加权的无监督域适应模型(Sample weighted and Class weighted based Unsupervised Domain Adaptation Network, SCUDAN)。具体而言,一方面,通过源域类层面的适应性加权来调整源域类权重,以实现源域与目标域之间的类分布对齐;另一方面,通过目标域样本层面的适应性加权来调整目标域样本权重,以实现目标域与源域类中心的对齐。此外,文中还提出了一种 CEM(Classification Expectation Maximization)优化算法,以实现 SCUDAN 的优化求解。最后,通过对比实验和分析,验证了所提模型和算法的有效性。

关键词: 无监督域适应;最大均值差异;类权重偏差;样例权重偏差;卷积神经网络

中图法分类号 TP391

Unsupervised Domain Adaptation Based on Weighting Dual Biases

MA Chuang¹, TIAN Qing^{1,2}, SUN He-yang¹, CAO Meng¹ and MA Ting-huai¹

1 School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China

2 National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

Abstract Unsupervised domain adaptation (UDA) is a new kind of machine learning paradigm, which facilitates the training of target domain model through transferring knowledge from source domain to unlabeled target domain. In order to model the domain distribution difference between the source domain and target domain, the maximum mean discrepancy (MMD) is widely applied, it plays an effective role in promoting the performance of UDA. Usually, the class size and data distribution between the target domain and the source domain are not the same, unfortunately, these methods usually ignore this structure information. To this end, this paper proposes a model called sample weighted and class weighted based unsupervised domain adaptation network (SCUDAN). On one hand, the class distribution alignment between the source domain and the target domain is achieved through adaptive weighting on the classes of the source domain. On the other hand, the class centers between the target domain and the source domain can be aligned through adaptive weighting on the samples of the target domain. In addition, a CEM (Classification Expectation Maximization) algorithm is proposed to optimize SCUDAN. Finally, the effectiveness of the proposed method is verified by comparative experiments and analysis.

Keywords Unsupervised domain adaptation, Maximum mean discrepancy, Class weight bias, Sample weight bias, Convolutional neural network

收稿日期:2020-07-06 返修日期:2020-08-15 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:国家自然科学基金(61702273);江苏省自然科学基金(BK20170956);江苏省高校自然科学研究面上项目(17KJB520022);中国科学院模式识别国家重点实验室开放课题(202000007);模式分析与机器智能工信部重点实验室开放课题(NJ2019010)

This work was supported by the National Natural Science Foundation of China(61702273), Natural Science Foundation of Jiangsu Province (BK20170956), Natural Science Foundation of the Jiangsu Higher Education Institutions of China(17KJB520022), Open Projects Program of Chinese Academy of Science National Laboratory of Pattern Recognition(202000007) and Open Project Program of MIIT Key Laboratory of Pattern Analysis and Machine Intelligence(NJ2019010).

通信作者:田青(tianqing@nuist.edu.cn)

1 引言

在传统的机器学习方法中,研究者通常直接将在训练域得到的模型直接应用到测试域上,该方法通常假设训练域与测试域遵循同一分布。事实上,由于样本采集方式、特征提取方式不同,测试域几乎不与训练域同分布,这导致了训练域的模型无法在测试域上得到良好的结果。不仅如此,随着深度学习的快速发展,当前模型对标记样本数量和质量的 demand 增大^[1],但现有的样本大多数是无标记的,且人工赋予样本合适的标签会浪费大量的精力。如何将有限标签样本中的相关知识转移到无标签样本中并完成标记,成为了当前亟需解决的问题。为了解决上述问题,一种新的迁移学习范式——域适应^[2-3]被提出。

当前,域适应已在多种场景中取得广泛的应用,如图像识别^[4-5]、目标检测^[6-7]、跨域分类^[8-9]等。在域适应学习中,研究者通常将训练样本空间和测试样本空间分别命名为源域和目标域,通常源域和目标域具有一定的数据分布差异。根据目标域的标记情况,域适应可分为半监督域适应(Semi-supervised Domain Adaptation)^[10-11]和无监督域适应(Unsupervised Domain Adaptation, UDA)^[12-13]。半监督域适应指目标域部分样本含有标签信息,无监督域适应指目标域样本完全无标记。事实上,UDA 更贴合实际情况,因此受到了更多的关注与研究。在当前的 UDA 中,研究者主要将 UDA 划分为 5 类,分别为样本权重自适应^[14-15]、特征自适应^[16-17]、模型自适应^[18-19]、深度网络自适应^[20-21]和对抗自适应^[22-23]。样本权重自适应指由于存在概率分布的差异而引起的源域样本与目标域样本的权重差异,通过对样本的权重进行重采样使源域和目标域遵循相同权重,以解决概率分布不同的问题。特征自适应指对源域和目标域进行公共的特征表示,从而完成对源域和目标域的分布矫正。模型自适应又称为分类器自适应,在考虑到概率分布不匹配的情况下通过学习一个通用的分类器来完成源域和目标域的分类任务。近年来,由于神经网络和对抗网络的兴起,深度网络自适应和对抗自适应相继被提出。深度网络自适应指通过深度网络提取特定于不同域任务的特征,从而解决域适应问题。深度神经网络具有强大的特征表示能力,通常深度模型只建立在单一域上,因此对于存在较大域漂移的域适应问题,深度域适应方法难以获取其通用的特征。对抗自适应来源于生成对抗网络,是一种通过训练鲁棒的深度神经网络生成像素级目标样本或特征级目标的有效方法,其本质是通过对抗性目标(如二进制域鉴别器)来最小化域间差异,从而解决域适应问题。本文主要研究无监督场景下的域适应问题。

在 UDA 中,最大均值差异^[24](Maximum Mean Discrepancy, MMD)是一种常用的解决域分布差异的方法,该算法旨在对齐源域和目标域的中心,以消除域分布差异。与此同时,大量的基于 MMD 的算法被提出。文献[25]将核 MMD 与多分类器相结合来解决域适应问题,同时其通过最大可学习性确保可以从域中学到强判别模型。文献[26]结合交叉熵损失、MMD 以及源域与目标域的相似度损失,构建了基于深度网络的 CCSA(Classification and Contrastive Semantic A-

lignment)域适应模型。文献[27]提出了一种新的对比适应网络(CAN)优化方法,该方法借助 MMD 明确地模拟了类内和类间的域差异,并借助分布对齐的方法消除了域差异。尽管该方法已经取得了巨大的成功,但是现有的方法通常忽略了类权重偏差和样本权重偏差,然而这两类偏差对域适应来说是普遍存在的,且极易被样本选取标准和应用场景影响。图 1 和图 2 分别给出了类权重偏差和样本权重偏差的具体含义。图 1(a)和图 1(b)解释了不同的域类权重基本不同,这给域适应增加了难度。图 2(a)和图 2(b)分别给出了未考虑样本权重偏差的目标域类中心与考虑了样本权重偏差的目标域类中心,从图中可看出,考虑了样本权重后的类中心显然更为精确。为解决权重偏差影响域适应的问题,本文提出了一种基于权重自适应的 MMD 损失,通过表示目标域中的类权重和样本权重来实现域适应的目的。由于域适应问题中的目标域标签未知,其对应的类权重和样本权重未知,因此我们首先利用公共的分类器对目标域赋予伪标签,然后对目标域权重进行改写,使其保持与源域共享同类权重。随后,在条件 MMD(Conditional Maximum Mean Discrepancy, CMMD)中,基于空间距离对目标域样本权重进行改写,以更好地修正目标域在特征空间的类中心,从而实现权重估计与模型参数学习的联合优化。基于上述研究,本文结合现有的 CNN 架构,提出了新的域适应网络 SCUDAN。

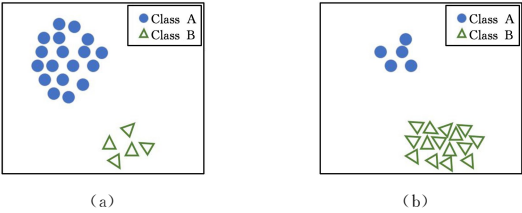


图 1 不同类的样本数量差异引起的类权重差异
Fig. 1 Difference of class weight caused by difference of sample number of different classes

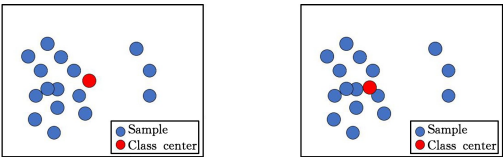


图 2 不同的样本权重差异引起的类中心差异(电子版为彩色)
Fig. 2 Difference of class center caused by difference of sample weight

本文的主要贡献如下:
(1) 本文在 MMD 和 CMMD 的基础上,提出了一种更为有效的损失 SCMMMD (Sample weighted and Class weighted MMD),重新修订了类权重与样本权重,从而更合理地改变了域中心和类中心,能够更好地消除域差异。
(2) 结合 SCMMMD 损失和经验损失,本文提出了无监督域适应网络 SCUDAN (Sample weighted and Class weighted

based Unsupervised Domain Adaptation Network),该网络可有效解决域适应问题。不仅如此,本文利用 CEM 原理训练该网络,得到了良好的结果。

(3)本文通过大量实验验证了 SCMMMD 在域适应方面优于 MMD,同时本文在不同的 CNN 特征提取器上和不同的数据集上依次验证了本文方法的优越性。

本文第 2 节介绍了域适应的常用方法以及平衡分布域适应算法;第 3 节介绍了基于权重偏差的两种 MMD 损失,即基于类权重偏差的 CWMMMD(Class Weight bias MMD)和基于样本权重偏差的 SWMMMD(Sample Weight bias MMD),并结合卷积神经网络构建域适应网络 SCUDAN;第 4 节给出了实验设置、方法对比和结果分析;最后总结全文。

2 相关工作

本节主要回顾最大均值差异 MMD 及条件最大分布差异 CMMD,并介绍了结合 MMD 与 CMMD 的平衡分布域适应(Balanced Distribution Adaptation, BDA)。

2.1 最大均值差异 MMD

域适应的目的是将从源域学习到的带有判别信息的模型自适应到目标域中,基于现有的研究分类,研究者根据目标域含有的标签数量将域适应分为 3 类:监督域适应(目标域样本完全含有标签)、半监督域适应(目标域样本不完全含有标签)、无监督域适应(目标域样本完全不含有标签)。本文重点解决无监督域适应问题。事实上,相比前两种域适应方法,无监督域适应更贴合实际生活场景。

无监督域适应面临的最大挑战是缺失的目标域标签将加大目标域分布的认知难度。为了解决这个问题,研究者通常选择消除域分布差异来实现无监督域适应。MMD 作为一种有效的无参消除域差异的方法,已经在域适应问题上取得了良好的结果。假定源域分布为 s ,目标域分布为 t ,通过映射 $\phi(\cdot)$ 将源域和目标域的样本同时转移到再生核希尔伯特空间(Reproducing Kernel Hilbert Space, RKHS)^[2],此时源域分布 s 和目标域分布 t 间的最大分布差异被表示为:

$$MMD^2(s, t) = \sup_{\|\varphi\|_{\mathcal{H}} \leq 1} \|E_{x' \sim s}[\varphi(\phi(x'))] - E_{x' \sim t}[\varphi(\phi(x'))]\|_{\mathcal{H}}^2 \quad (1)$$

其中, $E_{x' \sim s}[\cdot]$ 代表源域分布 s 的数学期望, $E_{x' \sim t}[\cdot]$ 代表目标域分布 t 的数学期望。 $\|\varphi\|_{\mathcal{H}} \leq 1$ 代表在 RKHS 球面空间内定义的映射规则。显然,当源域和目标域同分布,即 $s = t$ 时, $MMD^2(s, t) = 0$ 。假设源域表示为 $\mathcal{D}_s = \{x_i^s, y_i^s\}_{i=1}^M$, 目标域表示为 $\mathcal{D}_t = \{x_i^t\}_{i=1}^N$, 其中源域和目标域分别独立同分布于 s 和 t , 此时式(1)可重定义为:

$$MMD(\mathcal{D}_s, \mathcal{D}_t) = \left\| \frac{1}{M} \sum_{i=1}^M \phi(x_i^s) - \frac{1}{N} \sum_{j=1}^N \phi(x_j^t) \right\|_{\mathcal{H}}^2 \quad (2)$$

其中, M 和 N 分别代表源域样本数和目标域样本数; $\phi(\cdot)$ 代表样本核化下的特征图。

2.2 条件均值最大差异 CMMD

单一的 MMD 无法获得较好的域适应结果,其原因是在无监督域适应中,源域带有标签而 MMD 并没有有效利用此类标签。为此,部分利用源域标签的域适应算法被提出。其中应用最广泛的为条件 MMD,通常 CMMD 的表示如下:

$$\begin{aligned} CMMD(\mathcal{D}_s, \mathcal{D}_t) &= CMMD(P(y_s | x_s), P(y_t | x_t)) \\ &= \sum_{c=1}^C \left\| \frac{1}{n_c} \sum_{x_{s_i} \in \mathcal{Q}_s^{(c)}} \phi(x_{s_i}) - \frac{1}{m_c} \sum_{x_{t_j} \in \mathcal{Q}_t^{(c)}} \phi(x_{t_j}) \right\|_{\mathcal{H}}^2 \end{aligned} \quad (3)$$

其中, C 代表源域类数, y_u 代表对应样本 x_u 的标签, $u = s, t$ 。未特殊说明的场景中,默认目标域类等同于源域类。 n_c 和 m_c 分别代表源域对应类的样本数和目标域对应类的样本数。相比 MMD, CMMD 的优点在于成功利用了源域样本标签。利用标签的监督信息辅助域对齐也是目前最为主流的域适应研究方向。为此,文献[28]在 CMMD 的基础上提出了平衡分布域适应(Balanced Distribution Adaptation, BDA),其表达式如下:

$$\begin{aligned} D(\mathcal{D}_s, \mathcal{D}_t) &\approx (1 - \mu) \left\| \frac{1}{N} \sum_{i=1}^N \phi(x_{s_i}) - \frac{1}{M} \sum_{j=1}^M \phi(x_{t_j}) \right\|_{\mathcal{H}}^2 + \\ &\quad \mu \sum_{c=1}^C \left\| \frac{1}{n_c} \sum_{x_{s_i} \in \mathcal{Q}_s^{(c)}} \phi(x_{s_i}) - \frac{1}{m_c} \sum_{x_{t_j} \in \mathcal{Q}_t^{(c)}} \phi(x_{t_j}) \right\|_{\mathcal{H}}^2 \end{aligned} \quad (4)$$

BDA 结合了 MMD 的域差异消除的特点,并有效结合了源域标签,利用此监督信息实现了更优的域适应方案。尽管如此,现有研究表明忽略类权重偏差会降低域自适应的性能。事实上,现有的 MMD 方法默认源域类权重等同于目标域类权重。在存在类权偏差的情况下,借助源域的监督性对类偏差进行纠正以保持域不变性是可行且有效的做法。因此,本文将利用监督性信息纠正类偏差以实现域适应。

3 本文方法

本节将介绍基于类权重加权的最大分布差异 CWMMMD 和基于样例加权的最大分布差异度量 SWMMMD,并基于这两种度量方式设计基于样例和类联合重加权的域适应网络 SCUDAN。

3.1 基于类加权的最大分布差异

假设源域样本表示为 x_s , 目标域样本表示为 x_t , 同时假设 $p_s(x_s)$ 和 $p_t(x_t)$ 分别代表源域样本和目标域样本在训练后被正确分类的可能性。事实上, $p_s(x_s)$ 和 $p_t(x_t)$ 可以进一步理解为各样本的类条件混合分布,其表达式如下:

$$\begin{aligned} p_u(x^u) &= \sum_{c=1}^C p_u(y^u = c) p_u(x^u | y^u = c) \\ &= \sum_{c=1}^C \omega_c^u p_u(x^u | y^u = c), u \in \{s, t\} \end{aligned} \quad (5)$$

其中, $\omega_c^s = p_s(y^s = c)$ 且 $\omega_c^t = p_t(y^t = c)$, 它们分别代表源域和目标域的先验概率,即源域和目标域的先验权重。在理想情况下,当 $\omega_c^s = \omega_c^t$ 时,我们认为源域和目标域之间无类分布差异,此时的域适应效果最优。然而,在一般情况下,由于目标域的标记未知,且源域和目标域遵循不同分布,因此很容易出现 $\omega_c^s \neq \omega_c^t$ 。由于现有的 MMD 算法在计算类中心的过程中,完全忽略了源域和目标域的先验差异,因此 MMD 算法很难实现类偏差场景下的域适应。为了解决此问题,本文在 MMD 的基础上,结合类权重对域样本中心进行重定义,提出了基于类权重偏差的 MMD(Class Weight bias MMD, CWMMMD),其损失项的具体表达式如下:

$$CWMMD^2(\mathcal{D}_s, \mathcal{D}_t) = \left\| \frac{1}{\sum_{i=1}^M \alpha_{y_i^s}} \sum_{i=1}^M \alpha_{y_i^s} \phi(\mathbf{x}_i^s) - \frac{1}{N} \sum_{j=1}^N \phi(\mathbf{x}_j^t) \right\|_{\mathcal{H}}^2 \quad (6)$$

其中, $\alpha_{y_i^s}$ 表示第 i 个样本所在的源域与目标域的分类权重比值, 即 $\alpha_c = w_c^s / w_c^t$, 此式的作用是平衡源域与目标域之间的类权重, 即 $\alpha_c w_c^s = w_c^t$, 从而更有利于减小域分布差异。

3.2 基于样例加权的条件最大分布差异

第 2 节提到, CMMD 也是消除域差异的有效手段之一, 但与 MMD 一样, CMMD 在类中心对齐的过程中对样本权重考虑欠缺, 同样导致在域适应的过程中类中心不匹配。为了解决这个问题, 我们同样在 CMMD 中加入了相应的权重。原 CMMD 的表达式如下:

$$CMMD(\mathcal{D}_s, \mathcal{D}_t) = \sum_{c=1}^C \left\| \frac{1}{n_c} \sum_{\mathbf{x}_{ij} \in \mathcal{Q}_c^{(s)}} \phi(\mathbf{x}_{ij}) - \frac{1}{m_c} \sum_{\mathbf{x}_{ij} \in \mathcal{Q}_c^{(t)}} \phi(\mathbf{x}_{ij}) \right\|_{\mathcal{H}}^2 \quad (7)$$

其中, 由于各类样本数量已明确, 类权重信息已包含在类中心信息中。但是, 由于目标域无监督, 此时目标域的各类中心均由伪标签确定, 然而伪标签的不确定性将极大地扰动类中心的位置。不仅如此, 假设在第 k 轮更新中, 目标域类中心为 $\mathbf{x}_c^{(k)}$, 在所有类标签为 c 的目标域样本中, 必然有靠近类中心的样本和远离类中心的样本, 显然越靠近类中心的样本的置信度越高, 而在 CMMD 中, 各个样本的置信度相同, 这显然是不合理的。为此, 本文根据目标域样本到初始类中心的距离, 对每个样本进行权重重定义, 最终基于样本权重偏差的 MMD 损失 (Sample Weight bias MMD, SWMMMD) 的表达式如下:

$$SWMMMD(\mathcal{D}_s, \mathcal{D}_t) = \sum_{c=1}^C \left\| \frac{1}{n_c} \sum_{\mathbf{x}_{ij} \in \mathcal{Q}_c^{(s)}} \phi(\mathbf{x}_{ij}) - \frac{1}{\sum_{\mathbf{x}_{ij} \in \mathcal{Q}_c^{(t)}} \alpha_{ij}} \sum_{\mathbf{x}_{ij} \in \mathcal{Q}_c^{(t)}} \alpha_{ij} \phi(\mathbf{x}_{ij}) \right\|_{\mathcal{H}}^2 \quad (8)$$

其中, $\alpha_{ij} = e^{-\|\mathbf{x}_{ij} - \bar{\mathbf{x}}_c\|^2}$, $\bar{\mathbf{x}}_c$ 代表上一轮迭代过程中样本所属的类中心。通过调整样本权重, SWMMMD 能够有效修正目标域类中心, 从而达到消除域差异的目的。

3.3 域适应模型的建立

本文提出了 CWMMMD 和 SWMMMD 两种基于不同加权方法的最大分布差异度量模型。但是这两种方法显然无法直接应用在域适应问题中。一种直接的利用方式是接入深度网络, 替换原网络中的分类器。除此之外, 由于目标域完全无标签, 此时目标域分布几乎未知且类权重与类中心未知。为了解决此问题, 本文提出一种基于样例和类联合重加权的域适应网络 (Sample weighted and Class weighted based Unsupervised Domain Adaptation Network, SCUDAN)。该网络的本质是融合了本文提出的最大分布差异损失和 CNN 特征提取网络。

首先, 随着 CNN 网络层次向上, 提取的特征开始特定于任务, 导致数据集对更高层次特征的偏好增加。因此, 本文决定在 CNN 的更高层加入 MMD 正则化项, 并结合无监督学习建立域适应网络。最终网络模型正则化的函数表达式如下:

$$\min_{\mathbf{W}, \{\hat{y}_j\}_{j=1}^N} \frac{1}{M} \sum_{i=1}^M \ell(\mathbf{x}_i^s, y_i^s; \mathbf{W}) + \lambda CWMMMD(\mathcal{D}_s, \mathcal{D}_t) + (1 - \lambda) SWMMMD(\mathcal{D}_s, \mathcal{D}_t) \quad (9)$$

其中, $\mathbf{W}$ 代表模型待学习的模型参数, λ 代表超参数, $\mathcal{D}_s, \mathcal{D}_t$ 分别代表从源域和目标域中提取出的特征。类权重和样本权重将由目标域的分类结果来判定。式(9)中, 首项在源域上采用 softmax 损失, 后两项则是考虑了不同权重信息的 MMD 正则化项。最终, 目标域将通过源域参数模型 $\mathbf{W}$ 进行分类。

随后, 本文利用分类期望最大理论 (Classification Expectation Maximization, CEM)^[29] 来优化本文模型。优化步骤主要分为 3 步。

(1) E-Step. 假定模型已学习到模型参数 $\mathbf{W}$, 则通过此模型参数可以有效得到目标域样本的分类输出结果 $g_c(\mathbf{x}_j^t; \mathbf{W})$, 即:

$$p(y_j^t = c | \mathbf{x}_j^t) = g_c(\mathbf{x}_j^t; \mathbf{W}) \quad (10)$$

(2) C-Step. 此时, 目标域样本的类标签则是输出结果所属概率最大的类, 即:

$$\hat{y}_j = \arg \max_c p(y_j^t = c | \mathbf{x}_j^t) \quad (11)$$

此时利用类标签分别计算目标域的分类权重与类中心, 从而进一步得到各个样本的距离权重。

(3) M-Step. 固定类权重 α_c 与样本权重 α_{ij} , 此时模型参数 $\mathbf{W}$ 可表示为:

$$\min_{\mathbf{W}} L(\mathbf{W}) = \frac{1}{M} \sum_{i=1}^M \ell(\mathbf{x}_i^s, y_i^s; \mathbf{W}) + \lambda CWMMMD(\mathcal{D}_s, \mathcal{D}_t) + (1 - \lambda) SWMMMD(\mathcal{D}_s, \mathcal{D}_t) \quad (12)$$

式(12)可通过梯度下降求解。

SCUDAN 算法如算法 1 所示。

算法 1 SCUDAN 算法

输入: 源域样本 $\{\mathbf{x}_i^s, y_i^s\}_{i=1}^M$; 目标域样本 $\{\mathbf{x}_j^t\}_{j=1}^N$

输出: 目标域样本标签 $\{\hat{y}_j^t\}_{j=1}^N$

1. 利用 CNN 架构学习模型参数 $\mathbf{W}$;
2. For iteration = 1, 2, ..., iteration_{max}, do
3. 根据式(10)求得目标域分类结果 $g_c(\mathbf{x}_j^t; \mathbf{W})$;
4. 根据式(11)求得目标域样本标签 $\hat{y}_j$;
5. 优化式(12)得到模型参数 $\mathbf{W}$;
6. End for
7. 返回 $\hat{y}_j$, 此时 $\hat{y}_j$ 即为目标域标签。

4 实验

本节测试了本文提出的 SCUDAN 模型在 office10 + Caltech10 数据集以及数字识别数据集这两个基础数据集上的性能表现。此外, 本节还从参数敏感性的角度对所提模型和算法进行了验证和分析。

4.1 实验设置

遵循 UDA 的常见设置, 本文基于 4 种广泛使用的 CNN 网络实现 SCUDAN 模型, 即 LeNet^[30], AlexNet^[31], GoogLeNet^[32] 和 VGGnet-16^[33]。如文献[34]所述, 本文将基于预训练的 AlexNet, GoogLeNet 和 VGGnet-16 训练本文模型, 其中 AlexNet 固定 conv1 到 conv3 层, GoogLeNet 固定从 inc1 到 inc3 的起始层。此外, 目标域的所有类权重和样本权重均初始化为 1。本文将基于 SCMMMD 的正则化损失添加到 AlexNet 的最后 3 个全连接层、GoogLeNet 的最后 1 个初始层和全连接层以及 LeNet 的最后 1 个全连接层。本文所有深度模型均基于 Caffe 平台构建实现, 并且所有实验在配置

NVIDIA GTX 1660 GPU 和 16 GB 内存的计算平台上实现。所有实验的 *batch-size* 均设置为 32,超参数 λ 的取值范围为 $\{0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0\}$,且均经过五折交叉验证选取。所有实验的指标均为正确率±标准差(%)。

4.2 实验结果与分析

(1)Office-10+Caltech-10

Office-10+Caltech-10 被广泛用于域适应,其是从 Office-31 和 Caltech-256 中分别提取相同 10 个类形成的数据集。一般认为该数据集共包含 4 个域,分别是来自 Office-10 的 3 个类 Amazon(A),Webcam(W)和 DSLR(D),以及来自 Caltech-10 的 1 个类 Caltech(C)。在此数据集上,本文分别利用 AlexNet,GoogLeNet 和 VGGnet-16 衡量本文模型的有效性。本节将 SCMMD 与表 1 中的方法进行对比。为执行域适应任务,本文将预训练的 AlexNet,GoogLeNet 和 VGGnet-16 模

型作为特征提取器,并与不同的域适应模型相结合。LapC-NN^[35] 可认为是 CNN 的一个变种,它学习未标记数据特征并将其嵌入到深层结构中,并利用学习嵌入损失作为正则化器。DDC^[36] 在 CNN 结构中嵌入单核 MMD 层,建立统一的深度学习框架,共同学习语义特征和跨域性能。表 1 列出了本文方法与其他方法的对比结果。由表 1 可得:1)本文模型在不同的 CNN 结构框架中都得到了最优的平均结果,且在大部分实验中得到了最优的结果;2)本文模型得到了最低的标准差,相比其他方法,本文模型可以在大部分场景中得到最稳定的分类结果;3)作为同样考虑了不同域中权重偏差的方法,WDAN^[37] 在各个实验场景中得到了次优的方法,这说明将权重知识考虑进域适应场景中是有效且必要的。尽管本文方法相比 WDAN 提升不显著,但由于 WDAN 所处场景是半监督域适应场景,相应地,域适应难度低于 UDA,因此从该层面上看本文方法依旧具有明显的优势。

表 1 不同的基于 AlexNet,GoogLeNet 和 VGGnet-16 的方法在 Office-10+Caltech-10 上的结果

Table 1 Results of different methods based on AlexNet,GoogLeNet and VGGnet-16 on Office-10+Caltech-10 (单位:%)

Method	A→C	W→C	D→C	C→A	C→W	C→D	Avg
AlexNet	84.0±0.3	77.9±0.4	81.0±0.4	91.3±0.2	83.2±0.3	89.1±0.2	84.0
LapCNN(AlexNet)	83.6±0.6	77.8±0.5	80.6±0.4	92.1±0.3	81.6±0.4	87.8±0.4	83.9
DDC(AlexNet)	84.3±0.5	76.9±0.4	80.5±0.2	91.3±0.3	85.5±0.3	89.1±0.3	84.6
DAN(AlexNet)	86.0±0.5	81.5±0.3	82.0±0.4	92.0±0.3	92.6±0.4	90.5±0.2	87.3
WDAN(AlexNet)	86.9±0.1	84.1±0.2	83.9±0.1	93.1±0.2	93.6±0.2	93.4±0.2	89.2
SCUDAN(AlexNet)	87.2±0.1	84.8±0.1	84.3±0.1	93.2±0.1	93.9±0.2	93.5±0.2	89.4
GoogLeNet	91.3±0.2	88.2±0.3	88.9±0.3	95.2±0.1	92.5±0.2	94.7±0.3	91.8
DDC(GoogLeNet)	91.4±0.2	88.7±0.3	89.0±0.4	95.3±0.2	93.0±0.1	94.9±0.4	92.1
DAN(GoogLeNet)	91.4±0.3	89.7±0.2	89.1±0.4	95.5±0.2	93.1±0.3	95.3±0.1	92.3
WDAN(GoogLeNet)	91.5±0.2	91.7±0.3	89.8±0.3	95.7±0.4	93.5±0.3	96.0±0.3	93.0
SCUDAN(GoogLeNet)	91.5±0.1	92.0±0.2	90.1±0.3	95.7±0.4	93.4±0.3	96.1±0.2	93.1
VGGnet-16	89.6±0.4	88.1±0.4	85.4±0.5	93.7±0.2	94.3±0.2	93.7±0.2	90.8
DAN(VGGnet-16)	91.2±0.2	90.6±0.3	87.1±0.4	95.7±0.2	95.3±0.3	94.7±0.1	92.4
WDAN(VGGnet-16)	91.4±0.2	91.0±0.2	89.0±0.3	95.7±0.1	95.8±0.2	95.9±0.3	93.1
SCUDAN(VGGnet-16)	91.5±0.2	91.1±0.2	89.2±0.3	95.7±0.1	95.6±0.2	96.0±0.2	93.1

(2)数字识别数据集

本文在数字识别数据集上进行了域适应实验。本实验仅考虑了 MNIST(M),SVHN(S)和 USPS(U) 3 个基准训练图像域上的域适应。由于 LeNet 在数字识别上有较为出色的表现,因此将 LeNet 作为基准算法,其他算法将利用 LeNet 作为 CNN 架构,并在相应任务上进行域适应。SA 作为一种子空间对齐域适应方法,也将作为对比方法。表 2 列出了在数字识别数据集上的域适应结果。

表 2 不同方法在数字识别数据集上的结果

Table 2 Results of different methods on digit recognition dataset (单位:%)

Method	M→S	S→M	M→U	U→M	Avg
LeNet	17.2±0.3	56.8±0.5	61.5±0.4	46.5±0.6	45.5
SA	21.1±0.2	59.3±0.3	55.0±0.4	51.6±0.6	46.8
DAN	19.3±0.4	65.2±0.3	69.1±0.5	60.5±0.7	53.5
WDAN	23.5±0.3	67.3±0.5	72.3±0.4	65.5±0.5	56.4
SCUDAN	24.8±0.3	67.8±0.5	73.0±0.4	65.3±0.4	57.7

从表 2 中可以得出如下结论:1)尽管 LeNet 在数字识别数据集上具有不错的性能,但随着应用场景更加复杂和域适应任务难度的增加,LeNet 已经无法在当前场景中保持优秀

的表现;2)SCUDAN 在大部分场景中得到了最优结果,并比次优的 WDAN 整体提升了 1.7%,这证明了考虑样本偏差权重后,域适应结果会得到较大的提升;3)相比其他算法,SCUDAN 有着最小的标准差,这说明了 SCUDAN 可以得到最为稳定的实验结果。

4.3 参数敏感性分析

SCUDAN 仅包含一个参数 λ 。本节将对此参数进行敏感度分析,实验结果如图 3 所示。其中横坐标代表训练轮数,每轮训练取 10 次中间值,最终汇总出不同损失变化曲线。

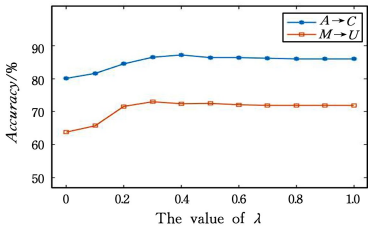


图 3 参数 λ 的敏感性

Fig. 3 Sensitivity of hyperparameter λ

由图 3 可以得到如下结论:1)在不同的数据集上,域适应任务 A→C 和 M→U 都在 $\lambda=0.3$ 左右取得了最优结果,这说

明基于类权重偏差损失的 MMD 和基于样本权重偏差损失的 CMMD 在不同程度上都提升了域适应的性能;2)当 $\lambda > 0.4$ 时,任务准确性开始出现轻微下降,这证明了样本权重偏差损失的重要性不及类权重偏差损失;3)当 $\lambda = 1$ 时,模型将退化成 DAN,这说明了本文方法明显优于 DAN,从侧面证明了 SCUDAN 的有效性。

4.4 收敛性分析

本节将通过实验证明本文方法的收敛性。在实验中, A→C 将作为分析模型收敛性的实验数据集。实验结果如图 4 所示,其中绿色线条表示 SCUDAN 的整体损失变化曲线,蓝色线条表示经验损失变化曲线,红色线条表示本文提出的 SWMMD 和 CWMMMD 损失和的变化曲线。从图 4 可以明显看出,随着迭代次数的增加,本模型的损失函数出现了明显的收敛,其中经验损失收敛最为明显。不仅如此,MMD 损失占整体损失的权重较大,这也从侧面说明了 MMD 损失的重要性。

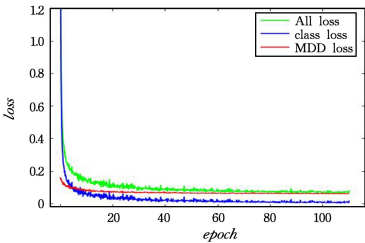


图 4 SCUDAN 在 A→C 上的收敛性(电子版为彩色)
Fig. 4 Convergence efficiency of SCUDAN on A→C

4.5 显著性分析

为了测试本文方法相比其他方法是否具有显著性,本文将在 A→C 上添加额外的 Friedman 检验测试,其中所有被检验的方法都以 AlexNet 网络为深度架构。测试结果如图 5 所示,其中各方法对应的数字排名表示其性能的优越性,数值越小代表方法的性能越优。此外,图 5 中处于不同线段的方法表示具备性能差异显著性,而处于相同线段的方法表示不具备性能差异显著性。从图中可以看出,本文方法不仅在结果上优于其他方法,而且具有较好的性能显著性。

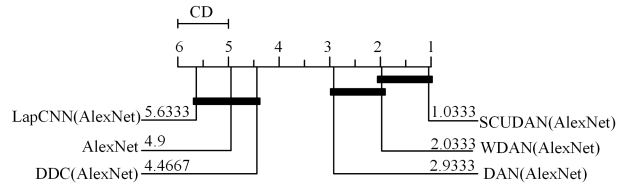


图 5 在 A→C 上的 Friedman 测试
Fig. 5 Friedman test on A→C

结束语 本文从域分布对齐的角度分析了权重偏差对域适应性能的影响,进而结合源域和目标域中各项不同的权重,分别提出了基于类权重偏差的 CWMMMD 损失和基于样本权重偏差的 SWMMD 损失,并结合 CNN 架构搭建了完整的域适应模型 SCUDAN。其次,本文利用了 CEM 算法,通过分配伪标签,调整类权重、样本权重,更新模型参数来优化本文提出的网络。实验结果表明,SCUDAN 在诸多域适应场景中有着良好的表现,并且显著优于未考虑先验知识的域适应网络 DAN。在后续研究中,我们将着重研究:1)在非 CNN 架构中

引入先验知识将对模型产生何种影响;2)如何更精确地描述权重偏差。

参 考 文 献

[1] LAWRENCE S, GILES C L, TSOI A C, et al. Face recognition: A convolutional neural-network approach[J]. IEEE Transactions on Neural Networks, 1997, 8(1): 98-113.

[2] PAN S J, TSANG I W, KWOK J T, et al. Domain adaptation via transfer component analysis[J]. IEEE Transactions on Neural Networks, 2010, 22(2): 199-210.

[3] DAUMÉ III H. Frustratingly easy domain adaptation[J]. arXiv: 0907.1815, 2009.

[4] SUN D M, ZHANG F F, MAO Q R. Label-Guided Domain Adaptation Method in Generative Adversarial Network for Facial Expression Recognition[J]. Computer Engineering, 2020, 46(5): 267-273, 281.

[5] WANG G, HAN H, SHAN S, et al. Unsupervised Adversarial Domain Adaptation for Cross-Domain Face Presentation Attack Detection[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 56-69.

[6] DUAN J M, MA X Z, LIU X. Path Tracking Method of Unmanned Vehicle Based on MFAPC[J]. Computer Engineering, 2019, 45(6): 6-11.

[7] INOUE N, FURUTA R, YAMASAKI T, et al. Cross-domain weakly-supervised object detection through progressive domain adaptation[C] // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018: 5001-5009.

[8] CHEN C, GUO W B, LI Q Y. Adversarial domain adaptation with self-attention in image classification[J]. Computer Engineering and Science, 2020, 42(2): 259-265.

[9] SAITO K, KIM D, SCLAROFF S, et al. Semi-supervised domain adaptation via minimax entropy[C] // Proceedings of the IEEE International Conference on Computer Vision, 2019: 8050-8058.

[10] DAUMÉ III H, KUMAR A, SAHA A. Frustratingly easy semi-supervised domain adaptation[C] // Proceedings of the 2010 Workshop on Domain Adaptation for Natural Language Processing. Association for Computational Linguistics, 2010: 53-59.

[11] KUMAR A, SAHA A, DAUME H. Co-regularization based semi-supervised domain adaptation[C] // Advances in Neural Information Processing Systems, 2010: 478-486.

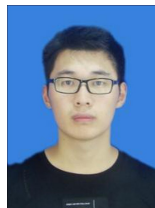
[12] FERNANDO B, HABRARD A, SEBBAN M, et al. Unsupervised visual domain adaptation using subspace alignment[C] // Proceedings of the IEEE International Conference on Computer Vision, 2013: 2960-2967.

[13] GANIN Y, LEMPITSKY V. Unsupervised domain adaptation by backpropagation[J]. arXiv: 1409.7495, 2014.

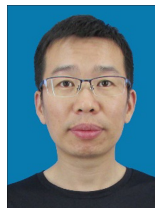
[14] JIANG J, ZHAI C X. Instance weighting for domain adaptation in NLP[C] // Proceedings of the 45th Annual Meeting of the Association of Computational Linguistics, 2007: 264-271.

[15] CHEN Q, LIU Y, WANG Z, et al. Re-weighted adversarial adaptation network for unsupervised domain adaptation[C] // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018: 7976-7985.

- [16] LIU J,ZHANG L. Optimal projection guided transfer hashing for image retrieval[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2019,33:8754-8761.
- [17] LONG M,WANG J,DING G,et al. Transfer feature learning with joint distribution adaptation[C]// Proceedings of the IEEE International Conference on Computer Vision. 2013:2200-2207.
- [18] DUAN L,XU D,TSANG I W H,et al. Visual event recognition in videos by learning from web data[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 34(9):1667-1680.
- [19] CAO Y, LONG M, WANG J. Unsupervised domain adaptation with distribution matching machines[C]// Thirty-Second AAAI Conference on Artificial Intelligence. 2018.
- [20] LONG M, CAO Y, CAO Z, et al. Transferable representation learning with deep adaptation networks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 41(12):3071-3085.
- [21] LONG M,ZHU H,WANG J,et al. Deep transfer learning with joint adaptation networks[C]// Proceedings of the 34th International Conference on Machine Learning-Volume 70. 2017:2208-2217.
- [22] PINHEIRO P O. Unsupervised domain adaptation with similarity learning[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018:8004-8013.
- [23] ZHANG J,DING Z,LI W,et al. Importance weighted adversarial nets for partial domain adaptation[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018:8156-8164.
- [24] DZIUGAITE G K,ROY D M,GHAHRAMANI Z. Training generative neural networks via maximum mean discrepancy optimization[J]. arXiv:1505.03906,2015.
- [25] GONG B, GRAUMAN K, SHA F. Reshaping visual datasets for domain adaptation[C]// Advances in Neural Information Processing Systems. 2013:1286-1294.
- [26] MOTIHAN S,PICCIRILLI M,ADJEROH D A,et al. Unified deep supervised domain adaptation and generalization[C]// Proceedings of the IEEE International Conference on Computer Vision. 2017:5715-5725.
- [27] KANG G,JIANG L,YANG Y,et al. Contrastive adaptation network for unsupervised domain adaptation[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2019:4893-4902.
- [28] WANG J,CHEN Y,HAO S,et al. Balanced distribution adaptation for transfer learning[C]// 2017 IEEE International Conference on Data Mining (ICDM). IEEE,2017:1129-1134.
- [29] CELEUX G,GOVAERT G. A classification EM algorithm for clustering and two stochastic versions[J]. Computational statistics & Data analysis,1992,14(3):315-332.
- [30] AL-JAWFI R. Handwriting Arabic character recognition LeNet using neural network[J]. International Arab Journal of Information Technology,2009,6(3):304-309.
- [31] IANDOLA F N,HAN S,MOSKEWICZ M W,et al. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and < 0.5 MB model size[J]. arXiv:1602.07360,2016.
- [32] ZHONG Z,JIN L,XIE Z. High performance offline handwritten chinese character recognition using googlenet and directional feature maps[C]// 2015 13th International Conference on Document Analysis and Recognition (ICDAR). IEEE,2015:846-850.
- [33] SIMONYAN K,ZISSERMAN A. Very deep convolutional networks for large-scale image recognition[J]. arXiv:1409.1556,2014.
- [34] LONG M,CAO Y,WANG J,et al. Learning transferable features with deep adaptation networks[J]. arXiv:1502.02791,2015.
- [35] WESTON J,RATLE F,MOBAHI H,et al. Deep learning via semi-supervised embedding[M]// Neural networks: Tricks of the trade. Springer,Berlin,Heidelberg,2012:639-655.
- [36] TZENG E,HOFFMAN J,ZHANG N,et al. Deep domain confusion: Maximizing for domain invariance[J]. arXiv:1412.3474,2014.
- [37] YAN H,DING Y,LI P,et al. Mind the class weight bias: Weighted maximum mean discrepancy for unsupervised domain adaptation[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2017:2272-2281.



MA Chuang, born in 1996, postgraduate. His main research interests include machine learning and pattern recognition.



TIAN Qing, born in 1984, Ph.D, associate professor, postgraduate supervisor. His main research interests include machine learning and pattern recognition.