Abstract—Domain adaptation generalizes deep neural networks to new target domains under domain shift. Active domain adaptation (ADA) does so efficiently by allowing the learning model to strategically ask data annotation questions. The state-of-the-art active domain adaptation via clustering uncertainty-weighted embeddings (ADA-CLUE) uses uncertainty-weighted clustering to identify target instances for labeling. In this work, we carefully study how ADA-CLUE balances uncertainty and diversity during active learning. We compare the original ADA-CLUE with a variant that weights clusters by a constant instead of by the uncertainty, and confirm that constant-weighted clustering sampling outperforms ADA-CLUE at early stages due to its stability. We then merge constant-weighted sampling and uncertainty-weighted sampling with a threshold to get the best of the two worlds. The merged solution, called CLUE with a loop threshold, is shown to be an empirically better choice than the original ADA-CLUE.

Index Terms—domain adaptation, active learning

I. INTRODUCTION

When trained on large-scale datasets, deep convolutional neural networks learn representations that are generically useful across a variety of tasks and visual domains [1], [2]. However, collecting large amounts of labeled data from scratch is time-consuming and impractical. Therefore, our goal is to use a single large dataset to train models that generalize well to novel datasets and tasks.

Due to covariate shift [3], however, models generalize poorly to novel datasets and tasks. Therefore, we seek to use cheaper sources of labeled data to train models that generalize to real-world targets [4], [5]. Consider, for example, an image classifier trained on synthetic or semi-synthetic images, which are abundant and fully labeled but which inevitably follow distributions that do not reflect real images. For object recognition, we seek to adapt models trained on synthetic data to real-world datasets [6] such as the Cityscapes dataset [7].

To this end, researchers have proposed domain adaptation (DA), a new research area in machine learning [4], [5]. In this scenario, training and test sets are termed source and target domains, respectively. Domain adaptation generally involves using labeled source data to train a model that generalizes to a target domain by minimizing the difference between domain distributions.

Domain adaptation using labeled source data and unlabeled target data in the training phase is unsupervised domain adaptation (UDA). Although domain adaptation provides a good starting point, the performance of UDA methods often falls far behind their supervised counterparts [8], [9]. In such cases, adding labeled data from the target domain could translate to performance benefits. Active learning (AL) selects queries to retain the most useful data for training from a large unlabeled data pool. Whereas domain adaptation (DA) transfers knowledge from a label-rich source domain to an unlabeled target domain, AL queries labels to yield a small subset of the most relevant samples. To this end, a series of active domain adaptation (ADA) methods has been developed. Given labeled data in a source domain, unlabeled data in a target domain, and the ability to obtain labels for a fixed budget of target instances, we seek to select target instances for labeling and update the model’s representations to maximize performance on the target test set.

The traditional AL setting typically focuses on techniques to select samples to efficiently learn a model from scratch, rather than adapting a model under a domain shift. In traditional AL, labels are acquired for samples by committee [10], uncertainty [11]–[14], or representativeness [15]–[17]. Although traditional AL methods dramatically lower human annotation costs, they are impractical when collecting out-of-distribution test data [18], [19]. As neural networks are poorly calibrated, model uncertainty is not reliable [20]. Given such model miscalibration, high confidence scores do not imply a high likelihood of correctness; thus the sampled examples are not the most uncertain ones. On the other hand, the main difference between ADA and traditional AL is that the calibration of these estimates in the target domain depends on the degree of the domain shift. These limitations complicate deployment of traditional AL. The major challenge of ADA is thus the selection criterion under domain shift.

Prior ADA work [21]–[23] has also underscored the importance of identifying instances that are both uncertain and diverse. Active adversarial domain adaptation (AADA) [23] combines uncertainty with diversity measured by targetness under a learned domain discriminator. However, such targetness does not ensure that the selected instances are representative of the entire target data distribution (i.e., not outliers), or dissimilar to one another. Ash et al. [15] instead propose clustering in a hallucinated “gradient embedding” space.
However, this depends on distance-based clustering in high-dimensional spaces, which often leads to suboptimal results. The state-of-the-art method for ADA is active domain adaptation via clustering uncertainty-weighted embedding (ADA-CLUE) [22], which selects the instance closest to each cluster centroid under the uncertainty-weighted embedding of target instances and then optimizes a semi-supervised adversarial entropy loss to induce domain alignment, jointly capturing uncertainty and diversity for active DA.

In this work, we systematically design the new algorithm and package to analyze whether the quality of the uncertainty is important. We propose active domain adaptation via density-weighted uncertainty sampling (ADA-DWUS), a label acquisition strategy for active DA. We select effective target samples on the basis of their diversity as well as the classifier uncertainty for the domain adaptation task. First, the unlabeled target pool is grouped into clusters using the k-means++ algorithm [24]. We leverage this to select the most effective target samples from the diverse target pool obtained in the first step, for annotation by the oracle. Second, we note that the target samples which differ from the source domain are difficult to classify correctly. Thus, to facilitate domain adaptation, those target samples which are farther away from the source samples and are likely to be incorrectly labeled should be given greater weight. The intuition is that instances for which the classifier is uncertain (small margin) provide the most information for learning. Hence we propose weighting the margin term for difficult samples without explicitly using their predicted labels, which may be incorrect. ADA-DWUS empirically reaches state-of-the-art performance on active DA benchmarks.

We compare the proposed method ADA-DWUS with CLUE [22] and observe that uncertainty as estimated by the classifier suffers from large variance, leading to unreliable queries and thus uninformative instances. We address this problem using CLUE with a loop threshold as a simple solution: in the initial stage, we query target samples from constant-weighted clustering; samples that exceed the threshold are additionally weighted according to their uncertainty. In active DA, this produces sampling instances from regions of the feature space that are well-aligned across domains in the early stage. After a given number of iterations, we query the target samples from uncertainty-weighted clusters to ensure that the target samples are not drawn from well-aligned feature space across domains. We conduct empirical experiments to determine a threshold that yields the desired value, with results that attest the usefulness of our study and our proposed approach.

In summary:

- We propose a loop threshold method to improve uncertainty-weighted embedding clustering.
- We show the importance of the uncertainty quality, propose an ADA framework, and compare different active learning methods. Our code is available at https://github.com/HUTTON9453/Active-DA.
- We demonstrate the effectiveness of our method on three datasets: SVHN→MNIST, DomainNet, and Office-31.
- We benchmark the performance of state-of-the-art active learning methods on three different domain shifts, and find that uncertainty-based methods are unreliable in the early stages for active DA.

II. RELATED WORK

A. Notation and Problem Setup

Here we introduce the setup and notation used throughout the paper. We consider C-way classification, in which X and Y represent random variables for features and labels respectively, where Y = {0,...,C−1}. In active domain adaptation, we have a labeled source domain LS = {(Xs,Ys)}, an unlabeled target domain UT = {(XUt,YsUt)} and a labeled target domain LT = {(XLt,YsLt)} of size B which is much smaller than the size of unlabeled target domain. The goal is to generalize a model trained on the source domain using a selection of labels from the target domain. The task is to learn a function h : X → Y (a convolutional neural network (CNN) parameterized by θ) that achieves good prediction performance on the target. The probability of class label y according the model weights θ is denoted by p(y | x; θ).

Classical machine learning techniques showcase the incorporation of active learning for the DA scenario. Chattopadhyay et al. [25] use importance weighting and select target samples with larger distances between features while training using MMD. Su et al. [23] propose AADA, an active learning method that uses H-divergence and importance sampling to query target instances. In AADA, a domain discriminator Gd is learned to distinguish between source and target features obtained from an extractor Gf, in addition to a task classifier Gy. For active sampling, points are scored via the following importance weighting-based acquisition function (H denotes model entropy): \( s(x) = \frac{1−\exp(G_f(x))}{G_y(G_f(x))} \); the top B instances are selected for labeling. However, their criteria do not include the diversity of the overall data. Prabhu et al. [22] instead propose ADA-CLUE, a state-of-the-art uncertainty-weighted clustering method that identifies target instances for labeling that are both uncertain under the model and diverse in feature space. The uncertainty term is measured by the predicted entropy under the model.

We propose active domain adaptation via density weighted uncertainty sampling (ADA-DWUS), a variant of CLUE that calculates the target samples as the centroid of the each uniform cluster and then weights the margin corresponding to the target sample to select informative target samples. In comparison with CLUE, ADA-DWUS yields state-of-the-art performance. However, we observe that early-stage model miscalibration causes the uncertainty term to be uninformative. Therefore, we propose improving ADA-CLUE using a loop threshold to retain diversity in the early stage and then combine uncertainty with diversity over the iteration threshold; we show that this outperforms prior work on diverse shifts across multiple learning strategies.
III. MAIN APPROACH

Here we introduce the overall framework of active domain adaptation, after which we analyze CLUE and compare it with variants including the proposed ADA-DWUS. Finally, we describe how to use the loop threshold method with CLUE.

a) Active Domain Adaptation Framework: Although active learning and domain adaptation have been well-studied individually, active domain adaptation presents new challenges. It is difficult to determine which selection criterion under domain shift is the most sample-efficient. Another difficulty is how exactly to perform adaptation given these labeled data from the target domain.

The proposed approach queries the most informative samples from this unlabeled pool during the DA process at regular intervals. These queried samples and their labels provided by the oracle are the labeled target data for semi-supervised DA. Our package follows this framework to analyze the state-of-the-art CLUE.

b) CLUE with Loop Threshold: Prior work on active learning identifies instances based primarily on uncertainty and diversity. Here we revisit uncertainty and diversity in the CLUE setting.

c) Uncertainty in CLUE: It is essential to identify instances that provide the model with new information. CLUE uses predictive entropy to measure the corresponding uncertainty of the informativeness. For C-way classification, entropy is defined as

$$H(Y|x) = - \sum_{c=1}^{C} p(c \mid x; \theta) \ln p(c \mid x; \theta).$$

(1)

d) Diversity in CLUE: A parallel line of work in active learning involves sampling instances that are representative of the unlabeled pool of data. CLUE clusters deep embeddings of target data points weighted by the corresponding uncertainty of the target model and selects the nearest neighbors of the inferred cluster centroids for labeling. First, CLUE selects an initial pool of diverse unlabeled target samples from the dataset $U_T$ with weighted k-means++ [24]. The goal is to group target instances that are similar in the CNN feature space based on their informativeness ($H(Y|x)$) and to measure the density of a given data point $x$. Let $\{\mu_1, \mu_2, \ldots, \mu_B\}$ denote the corresponding centroid of each set. CLUE acquires labels for the nearest neighbors of each of the $B$ centroids:

$$X_{LT} = \{\text{NN}(\mu_b); b = 1, 2, \ldots, B\}.$$  

(2)

The problem here is that when learning from scratch, model uncertainty may be unreliable, leading to the sampling of less-informative points. We use variants of CLUE to demonstrate this problem in the following section.

e) Active Domain Adaptation via Density Weighted Uncertainty Sampling (ADA-DWUS): We motivate the sample selection criteria using the idea of density-weighted uncertainty sampling (DWUS) [26], which assumes that data points lying on the classification boundary are informative, and that higher-density samples lie close to the decision boundary. DWUS uses the following active selection criterion:

$$\arg \max_{i \in I_u} E[(\hat{y}_i - y_i)^2 | x_i] p(x_i),$$

(3)

where $E[(\hat{y}_i - y_i)^2 | x_i]$ and $p(x_i)$ are the expected error and density of a given data point $x_i$, respectively, and $I_u$ is the index for the unlabeled data. This formulation indicates that those points which have the largest contribution to the current classification error and lie close to the decision boundary are more informative. The expected error is the uncertainty-based selection criterion. Uncertainty is combined with the density of the underlying data to increase the diversity.

Unfortunately, applying this intuition to come up with a sample selection strategy is non-trivial, because the target data is mostly unlabeled and the empirical risk cannot be computed before annotation. We thus take advantage of the margin: To measure the uncertainty using the margin, the uncertainty criterion $Q_u(x)$ for each target sample $x$ is defined as

$$Q_u(x) = 1 - (\max_{i} \hat{y}_i - \max_{j \neq \arg \max \hat{y}_k} \hat{y}_j).$$

(4)

We use the negative margin since a smaller margin corresponds to higher uncertainty. We use the margin of the highest and second-highest probabilities in the predicted class distribution $\hat{y}$. The margin is preferred since it integrates the second-most probable class label in the uncertainty metric and thus reduces the error rate by defining a decision boundary.

Next, we measure the density of a given data point $x$ based on feature space coverage. We select an initial pool of diverse unlabeled target samples from the dataset $U_T$ with k-means++. In particular, given the unlabeled target data $U_T$, we initially group all the samples into $N_{\text{cluster}} = C$ clusters, where $C$ is the number of classes. The goal is to group target instances that are similar in the CNN feature space and measure the density of a given data point $x$. Let $\phi(x)$ denote the feature embeddings extracted from the model and let $\{\mu_1, \mu_2, \ldots, \mu_C\}$ denote the corresponding centroid of each set. We use the L2 distance $\sigma(x)$ from the corresponding centroid to measure $p(x)$ as

$$\sigma(x) = ||\phi(x) - \mu_k||^2.$$  

(5)

To jointly capture both diversity and uncertainty, the overall objective is

$$\arg \min_{i \in I_u} Q_u(x_i) \ast \sigma(x_i).$$  

(6)

Two components in this measure are interpreted as follows: diversity cue $\sigma(x_i)$ and uncertainty cue $Q_u(x_i)$. The diversity cue allows us to select unlabeled target data instances which are representative, while the uncertainty cue suggests data which the model cannot predict confidently and which is close to the decision boundary.
A. Comparison to CLUE variants

In Table I we compare the three conditions. We observe that constant-weighted cluster sampling outperforms uncertainty-weighted CLUE in the early stages, because at this point the model is not yet well-aligned across the source and target domains, and thus evaluations of the uncertainty for the target instances are unreliable. In contrast, after a few iterations, the model becomes more reliable under the weak distribution shift, at which point we add the uncertainty term to capture informative target instances as opposed to redundant instances. To ensure diversity, after clustering, we select representative instances (i.e., non-outliers).

B. CLUE with Loop Threshold

Let $t$ be a threshold value and $U$ be a weighted-uncertainty matrix. We consider an weight matrix $W$ based on the loop threshold:

$$
W = \begin{cases} 
  U & \text{loop}_{\text{cur}} > t \\
  \text{constant} & \text{otherwise}.
\end{cases}
$$

The core idea is to increase the credibility of the uncertainty so that we can identify informative instances for labeling. In general, we select $t$ as the loop threshold when the empirical performance of constant-weighted clustering sampling is better than that in CLUE. For example, increasing $t$ means more chances to query uninformative instances that are already well-aligned across domains; correspondingly, we expect diversity to play a bigger role. Similarly, at lower values of $t$ we expect uncertainty to have greater influence.

After querying labels data for $U_T$, we proceed to the next step of active domain adaptation: we train the model with labeled source and target data and unlabeled target data. We conduct experiments with three methods: 1) Fine-tuning the model on $L_T$; 2) Adversarial training via DANN [27] using $(L_S \cup L_T, U_T)$; and 3) Semi-supervised domain adaptation via minimax entropy [28] using $(L_S \cup L_T, U_T)$. We compare each query strategy in the different domain adaptation methods.

IV. EXPERIMENTS

For all experiments, we followed the standard flow of active domain adaptation, with multiple rounds of batch active sampling, label acquisition, and model updates. As our performance metric, we computed model accuracy on the target test split. We used a ResNet34 CNN and performed 10 rounds of active DA with a per-round budget of 500 instances (for a total of 5000 labels) for DomainNet and a budget of 30 instances (300 labels total) for Office31. In addition, we evaluated the performance on the SVHN $\rightarrow$ MNIST shift. We used a modified LeNet architecture, and performed 30 rounds of active adaptation with a per-round budget of 10. We evaluated the results on the standard benchmark datasets: DomainNet [29], DIGITS (SVHN [30] as the source domain and MNIST [31] as the target domain), and Office31 [4].

We compared with CLUE to show that the loop threshold yields improved performance. (1) CLUE [22] is a state-of-the-art active DA method for entropy-weighted clustering that selects diverse, informative target instances for labeling from dense regions of the feature space. (2) ADA-DWUS is our proposed variant of CLUE which clusters deep embeddings of target instances by uniform weighting and then selects the nearest neighbors of the inferred cluster centroids weighted by the corresponding uncertainty for labeling. By comparing these, we propose (3) CLUE with a loop threshold, which introduces threshold $t$ to control when to perform uncertainty clustering. We additionally compared with an active domain adaptation method: (4) AADA [23] is a hybrid active learning method for domain adaptation that uses a combination of the entropy measure from a classifier and the outputs of a domain discriminator. Target instances are selected based on the predictive entropy and targetness measured by an adversarial domain discriminator followed by adversarial domain adaptation via DANN. Furthermore, we compared the proposed approach with traditional active learning methods. Uncertainty-based sampling [14] includes (5) Entropy sampling, which selects samples with the highest predictive entropy, and (6) Margin sampling, which selects samples for which the score difference between the top-2 predictions is the smallest. We experimentally illustrate that traditional active learning methods which are based purely on uncertainty are ineffective because the uncertainty term is unreliable under domain shift. In terms of diversity-based sampling, we used (7) Core-set [17], which uses greedy k-center clustering to select samples from unlabeled data such that the largest distance between the remaining unlabeled data and labeled data is minimized. We show that this solely diversity-based method generalizes poorly under domain shift. Hence we also considered methods that combine uncertainty and diversity. (8) BADGE [15] is a hybrid deep active learning method that optimizes both uncertainty and diversity. The main difference between CLUE and BADGE is the embeddings for clustering. BADGE clusters gradient embeddings via KMeans++, whereas CLUE clusters penultimate-layer embeddings via KMeans++. Finally, (9) Random sampling selects samples uniformly at random. We take this as our baseline; this allows us to compare the benefit of active learning over passive learning.

We evaluated all query methods across three DA paradigms: (1) Fine-tuning from source: we trained the model using $L_S$ and then fine-tuned it on $L_T$, both in a supervised way. (2) MME from source: Minimax entropy (MME) [32] is a state-of-the-art semi-supervised DA method that starts from a model trained on $L_S$ that minimizes adversarial entropy loss for unsupervised domain alignment in addition to finetuning
on $L_S \cup L_T$. (3) DANN from source: DANN [27] is an adversarial method. We trained the classifier using $(L_S \cup L_T, U_T)$. Regardless of the DA paradigm, we show that the proposed method selects informative instances.

In summary, the proposed method addresses two questions: how to select images to label from $U_T$ to yield the greatest performance gain, and how to train a classifier given $\{L_S, L_T, U_T\}$. We conduct the following experiments to answer these questions.

V. RESULTS AND DISCUSSION

a) Comparison of Sampling Methods: We observe that CLUE with the loop threshold consistently outperforms the other methods. Pure uncertainty (margin, entropy) and diversity (core-set) methods work well with easy cases (Real $\rightarrow$ Clipart and SVHN $\rightarrow$ MNIST) (Table IV), but all are outperformed by random sampling. In contrast, the proposed method and other hybrid approaches perform favorably against these. Overall, our method consistently performs best. Averaged over four DomainNet scenarios (Table III), CLUE with the loop threshold outperforms margin-based uncertainty sampling and core-set diversity sampling at $B = 2k$ by 1.4% and 2.7% with fine-tuning, and 2.1% and 3.0% with MME adaptation.

However, across learning strategies, shifts, benchmarks, and most rounds, DWUS’s performance is within 1% of CLUE’s performance. These two methods use the same clustering method (K-means++) and are hybrid methods that combine uncertainty and diversity sampling. CLUE clusters deep embeddings of target instances weighted by the corresponding predictive entropy of the target model and then selects the nearest neighbors of the inferred cluster centroids for labeling. However, DWUS clusters deep embeddings and then weights these by the corresponding margin of the target model. Clearly, the main difference between DWUS and CLUE is the uncertainty term and whether clustering is weighted. We discuss this below.

Table II shows that constant weighting is better than uncertainty weighting at the early stage. This shows that the uncertainty measure is uninformative at the early stage.

b) Comparison of DA paradigms: We now evaluate our method’s compatibility with a few additional domain adaptation strategies from the literature. Across AL methods, we observe that MME adaptation consistently outperforms finetuning by 2.3%–4.4% accuracy on DomainNet.

c) Sensitivity to threshold $t$: In Figure 1, we conduct a sweep over the threshold values for CLUE with the loop threshold on Office31. As seen, CLUE with the loop threshold improves performance, particularly at later rounds when the number of labels from target data is about 3%. For example, in Figure 1, the best performance is obtained when the total number of instances of the target is 1886 and total number of labeled target instances via diversity sampling is 60. Thus, the ratio of the labeled target instances with diversity to the total number of target data instances is 3.2%. We select $t \ast B/(\text{total number of target data instances}) \approx 3\%$ as the default value.

VI. CONCLUSION AND FUTURE WORK

We propose active domain adaptation via density weighted uncertainty sampling (ADA-DWUS), a unified framework for active domain adaptation. When few labeled targets are available, the domain adaptation model improves classification while combining uncertainty and diversity to select the most informative samples from the target domain. We also propose CLUE with a loop threshold to account for miscalibration of the model uncertainty in the early stage. We show that our methods outperform the state-of-the art method for active DA.

ACKNOWLEDGMENTS

This work roots from the M.S. thesis of the first author [33]. We thank Profs. Yun-Nun Chen and Hung-Yi Lee for their valuable feedback. The work is partially supported by the Ministry of Science and Technology of Taiwan via the grants MOST 110-2628-E-002-013 and 111-2628-E-002-018. We also thank the National Center for High-performance Computing (NCHC) of National Applied Research Laboratories (NARLabs) in Taiwan for providing computational resources.

REFERENCES


