Uncertainty Reduction for Model Adaptation in Semantic Segmentation

Prabhu Teja S \textsuperscript{a,b} \quad François Fleuret \textsuperscript{a,c}

\textsuperscript{a}Idiap Research Institute, \textsuperscript{b}EPFL, \textsuperscript{c}University of Geneva

prabhu.teja@idiap.ch, francois.fleuret@unige.ch

Abstract

Traditional methods for Unsupervised Domain Adaption (UDA) targeting semantic segmentation exploit information common to the source and target domains, using both labeled source data and unlabeled target data. In this paper, we investigate a setting where the source data is unavailable, but the classifier trained on the source data is; hence named “model adaptation”. Such a scenario arises when data sharing is prohibited, for instance, because of privacy, or Intellectual Property (IP) issues.

To tackle this problem, we propose a method that reduces the uncertainty of predictions on the target domain data. We accomplish this in two ways: minimizing the entropy of the predicted posterior, and maximizing the noise robustness of the feature representation. We show the efficacy of our method on the transfer of segmentation from computer generated images to real-world driving images, and transfer between data collected in different cities, and surprisingly reach performance comparable with that of the methods that have access to source data.

1. Introduction

The successes of deep learning, especially in semantic segmentation, have been driven in large part by large architectures \cite{10, 9}. While architectural improvements have made tremendous strides in improving performance, these large computation machines require vast amounts of data to be trained adequately. A few large densely labeled datasets such as Cityscapes \cite{17}, or Berkeley Deep Drive \cite{73} exist, but producing them, for instance for a new use case due to a different environment, or sensors, is very laborious and expensive; Cordts et al. \cite{17} reports that each image required about 90 minutes for labeling and verification. Added to the difficulty of collecting data for segmentation, minor changes in conditions like change of cities between train and test results in a drop of performance \cite{15}, as so does change in lighting conditions \cite{19}, as it violates the pivotal assumption of test and train data being sampled from the same distribution \cite{57}. Thus, owing to the large costs, both time and economic, creating annotated datasets for each scenario is impractical, motivating the re-use or transfer of knowledge from available images to requisite application.

The problem of transfer for segmentation has been predominantly investigated in literature (see Section 4) in two settings: adapting a model trained on synthetically generated images to real images, and adapting a model to cities different than the ones it has been trained for. We too adopt these settings for study in this paper. The synthetic-to-real images adaptation has attracted a lot of attention as the cost of generating segmentation ground truth for graphically rendered frames like GTA \cite{58}, or Synthia \cite{60} is substantially lower. Richter et al. \cite{58} labeled a total of 24,966 frames at an average of 7 seconds per frame, a large drop from 90 minutes taken for Cityscapes. However, due the nature of their generation, these synthetic images have a significant domain gap to the real images, which results in a large drop in the performance of networks trained on synthetic data when they are used on real images. Similarly, given the existing real world datasets like Cityscapes, it is paramount that the knowledge learned on these datasets is effectively transferred to different scenarios, without having to provide annotated data for each scenario.

A large portion of the methods that has been devoted to tackling this problem, like some of the ones reviewed in Section 4, require the labeled source data to be available along with the unlabeled target data for the adaptation process. We, in this paper, focus on the problem where the source data itself is not available but the source trained classifier is \cite{16}. This is similar to life-long learning \cite{63}, where the goal is to adapt to several tasks over several domains, and the only information payload that is carried over is the model itself. Differing from that, we are not concerned with preserving the performance on the source task. The current problem of source data-less transfer is pertinent when there exist data sharing restrictions on the source data; a common way to circumvent this is to share the trained classifier from which the input data itself cannot be reconstructed. A classical application is in medical image processing, where patient data cannot be freely shared due to privacy concerns,
but a trained model can be. Another relevant application where we envisage such a setting is in search-and-rescue operations, where data is collected on a mobile drone, and the segmentor network is adapted based on only the data collected, without having the need to access the original labeled dataset. Thus the problem of domain adaptation in the absence of source data, termed model adaptation [16], is of practical significance.

In this work, we study the problem of model adaptation for semantic segmentation. To the best of our knowledge, ours is the first work to do so. In the absence of source labeled data that has been effectively exploited by previous works, we enforce auxiliary properties that are desirable in a system, namely confident predictions for the target data, and noise resilience, and thereby increased stability of classification to parameter choices. To this end, we propose a method that uses feature corruption [16, 47, 54], and entropy regularization [29, 69]. We find that having access only to the source classifier, along with unlabeled target data, can result in performance comparable to the case where source data is also available.

2. Handling the absence of labeled source data

2.1. A toy problem

To motivate our method, we consider the ideal case depicted on Figure 1. Let us consider a simple case of binary classification of \( Y = \{0, 1\} \) for a scalar input feature \( x \in \mathbb{R} \). The probability of classification is defined using a sigmoid function of the input \( x \) and a threshold \( t \)

\[
p(Y = 1|X = x; t) = \frac{1}{1 + e^{-(x-t)}}
\]  

(1)

For illustration in Figure 1, we show the class conditional distributions, though we do not use class information. With only the information of the feature distribution \( \mu_X(x) \), our goal is to reason about scenarios that are likely to generalize better. If the labels are available, traditional wisdom tells us that Figure 1c is likely the ideal scenario to attain in terms of generalization [62]. We make it a little more concrete here, in the case where the labels are not available.

In Figure 1a, the feature \( x \) is given by a source trained feature extractor, and \( t_S \) is the threshold learned. It is apparent that such a threshold is quite likely ill-suited for the target domain, as it places the decision boundary in a high density region of the feature space, contradicting the traditional cluster & continuity assumptions [7, 41, 6]. However, if we change the threshold to \( t_* \), we expect better generalization performance. Note that this is also the classifier for which the entropy of output probability predictions over the distribution \( \mu_X(x) \) is the lowest. We mathematically define this idea and show numerical simulations for these cases in Appendix B.

We would like to modify the feature extractor itself such that the class conditional distributions overlap lesser than in Figure 1a. This can be achieved by imposing an entropy penalty on output posterior predictions, and using that penalty to train the feature extractor too. We show this in Figure 1b. As the overlap of the class-conditional data distributions decreases, we expect the generalization performance to improve.

The ideal scenario is shown in Figure 1c, where a large number of thresholds can separate the two classes, and we choose one that results in the least uncertain predictions of target data. One can draw parallels to max-margin methods like the SVM, where one is interested in finding a separator that is optimally distant from all classes. In a nutshell, we see that a classifier that has stable predictions for a range of parameter choices is likely to generalize better. This is, of course, in our context where we do not have access to labeled training data. In order to accomplish this, we need to go beyond entropy quantification of the predicted labels; we enforce stability of predictions over noisy features \( x \pm \epsilon \).

2.2. Proposed method

We, first, formally define the problem. Let \( \mathcal{X} \in \mathbb{R}^D \) be the input, and \( \mathcal{Y} \in \{1 \ldots K\} \) the labels. Let \( S \) with density \( \mu_S(x) \) be the source domain and \( T \) with density \( \mu_T(x) \) be the target one, where we do not have access to the labels of \( T \) while training. Let \( X_S = \{(x_i, y_i) \ i = 1 \ldots N_s, x_i \sim \mu_S(x), y_i \sim p_S(y)\} \) be the source data, and \( X_T = \{(x_i, ) \ i = 1 \ldots N_t, x_i \sim \mu_T(x)\} \) the target data. Let \( p_T(y) \) be the target domain label prior that is unknown to us. Here \( \mu_S \neq \mu_T \). We do not have direct access to \( X_S \), but have access to a network trained on \( X_S \). Let us denote that network by \( f(x, \theta_S) \equiv f_S(x) \) where \( \theta_S \) denotes the parameters of the network trained on the source data. Let \( g \) and \( h \) denote the feature extractor and classifier respectively, whose composition is \( f = h \circ g \). Let also \( \theta_g \) and \( \theta_h \) be their corresponding parameters. In our case, the network \( g \) refers to the ResNet-101 backbone, and \( h \) refers to the ASPP [10] decoder, which we describe in Section 3.3. For convenience, \( h \) also subsumes the softmax layer, and thus \( f(x; \theta) = p(y|x; \theta) \), where \( y \) is a vector of probabilities from which the predicted label is sampled. Summarizing, we have \( f_s \) and \( X_T \), and our goal is to modify \( f_s \) such that its performance is improved on \( T \) data.

2.2.1 Optimizing the feature extractor to generate robust features

The likelihood of predictions \( y \) for an input of \( x \in T \) is computed by \( f(x; \theta) \), on which an entropy penalty can be imposed [29]. However, with a trivial application of this, for the illustration in Figure 1b, the network can learn to separate the distribution by placing the threshold \( t_s \) at an arbitrary point and shearing the feature distributions around
Shared Backbone—

Equations (2), (3) and (5). At test time, we discard the auxiliary branches, and thus there is no additional computation at inference.

Figure 1: Given only the feature distributions in 1a to 1c in a two-class scenario, which one generalizes the best? In 1a, we show the distribution of features extracted by source trained network and the corresponding source threshold on the target data. Tuning the threshold to $t_s$ from $t_g$ is expected to result in better generalization. If we can modify the feature extractor itself, reducing the uncertainty of classification over the domain gives us 1b. This can be achieved by penalizing the entropy of predictions of each of the data points. We argue that while entropy is seemingly sufficient, we need to reduce the uncertainty in the predictions of the network over a wide range of parameter choices obtain better separation of the data like in 1c, and thereby better generalization. Details in Section 2.1.

Figure 2: An illustration of the proposed method. The main decoder is trained with Equations (3) and (5), whereas the backbone feature extractor is trained with a combination of Equations (2), (3) and (5). At test time, we discard the auxiliary branches, and thus there is no additional computation at inference.

The proposed uncertainty loss in Equation (2) improves the noise resilience of the network. In addition to that we use an entropy regularizer that minimizes the entropy of the network without dropout. In such a case, we propose to compute the uncertainty loss as

$$\mathcal{L}_{un} = \frac{1}{N} \sum_{i=1}^{N} (\hat{y}^i - y)^2 \tag{2}$$

To implement Equation (2), we introduce dropout only between $g$ and $h$. In the context of Bayesian neural networks, such a method has been termed LastLayer-Dropout elsewhere [55]. Instead of using a single branch that predicts the output with dropout-weights, we use multiple decoders $h$ that takes in dropped out features predicted by $g$. Thus $y = f(x; \theta) = h(g(x; \theta_g); \theta_h)$ and $\hat{y} = f(x; \hat{\theta}) = \hat{h}(g(x; \theta_g); \hat{\theta}_h)$. Thus, each auxiliary decoder $h$ sees only partial feature tensor, and is required to come as close as to reconstructing the original label tensor. We, experimentally, find that freezing the main decoders’ weights $\theta_h$ while training the auxiliary decoders’ parameters $\hat{\theta}_h$ results in better performance. Our full method is shown in Figure 2.
network’s predictions, that results in better empirical performance.

\[ L_{\text{ent}} = H\{f(x; \theta)\} \quad (3) \]

where, \( H\{\} \) is the entropy of the probability distribution over all \( K \) classes for an input \( x \). We hypothesize that this is because the dropout noise modifies the decision boundary given by the optimizer itself, and thus is beneficial to explicitly regularize the predictions given that estimate of weights. We find that we do not need a diversity enforcing loss, as specified in [37, 44], to prevent degeneracies.

### 2.2.2 Regularizing using the source trained model

We note that the losses in Equations (2) and (3) do not use the information in the source trained classifier, but enforce certain properties to be satisfied by the network on the target domain. In Figure 1c, an interchanged labeling \( i.e., \) where class-0 is predicted class-1 and vice-versa, results in the same loss value for Equations (2) and (3). To avoid such issues, and to infuse plausible class structure to the data, we use pseudo-labeling.

Pseudo-labeling or self-training has been a mainstay method in the semi-supervised problems, prior to the deep learning era. However, owing to the availability of large-scale datasets, it has been used to great success [1, 41, 71] for several classification problems. Traditional methods use the class with the highest predicted probability as the ground-truth for each unlabeled sample. However, in the case of a domain change, the accuracy of such predicted pseudo-labels is low. So we use the following modification to the standard definition

\[ y_{PL} = \begin{cases} 
\arg \max f(x, \theta) & \text{if } \max(f(x, \theta)) \geq \tau \\
\text{IGNORE} & \text{otherwise}
\end{cases} \quad (4) \]

\( i.e., \) we only consider as pseudo-labels the samples that are at least \( \tau \) confident. The samples with the \text{IGNORE} label do not contribute to the loss. However choosing \( \tau \) is a non-trivial task, as too low a threshold will result in wrong labels, and too high a threshold will result in no target data being bootstrapped for training. In this work we adopt the strategy of class balanced thresholding [81], where \( \tau \) is varied per class, such that a certain proportion of points per class are always selected. We define the pseudo labeling loss to be the cross-entropy loss with the pseudo labels as defined in Equation (4)

\[ L_{PL} = -\mathbf{1}^T_{y_{PL}} \log(y) \quad (5) \]

where \( \mathbf{1}_{y_{PL}} \) is one-hot encoded vector of \( y_{PL} \), and \( \log \) is applied element-wise.

Thus, the overall loss function being optimized is the combination of Equations (2), (3) and (5):

\[ L = L_{PL} + \lambda_{\text{ent}} L_{\text{ent}} + \lambda_{\text{un}} L_{\text{un}} \quad (6) \]

where \( \lambda_{\text{ent}}, \lambda_{\text{un}} \) are the weights of the individual loss terms.

Our work is connected to recent work in interesting ways: if Equation (2) is construed to be a form of self-supervision, our method can be interpreted as a form of \textit{test-time training} [65]. \textit{Test-time training} proposes to use an auxiliary task at test-time that helps combat domain shift from the training set. We differ from them in that we do not update the network at test time, but do so when given target domain data. Similarly, our work, conceptually, uses self-supervision for domain adaptation, similar to [64], but doesn’t need access to source labeled data. Additionally, our method can be interpreted as a form of making the network a \textit{a bit Bayesian} [38], where instead of placing Gaussian posterior on the weights of the penultimate layer’s weights, we use dropout distribution. As previously mentioned, our method has similarities to pseudo-tasks, in multi-task learning [49], which uses labeled data for training.

### 3. Experiments

#### 3.1. A toy problem

To elucidate the utility of each of the terms in Equation (6), we use a toy problem as shown in Figure 3. In Figure 3 a & b we show the source and target datasets; we use a rotated version of the source data as the target data. As it is in our case, we do not use the labels of the target data. We train a small two layer neural network with batchnorm and ReLU activations. We provide the exact architecture in Table 5 in the appendix. We take the outputs before the last classifier layer as the features of the network, and use the techniques that we described in Section 2.2 to train the network, except we do not use pseudo labeling for this problem. We use a feature dimensionality of 2 and plot the target features in Figure 3c with the source classifier. It is very apparent that the source network extracts features that do not transfer well. In Figure 3d, with a simple entropy regularization on the target data, we see that the performance improves tremendously. However, some of the blue points are very close to the separating line. To remedy this, our proposed feature noise decoder (detailed in Section 2.2) pushes the points away from the separating line. This can be interpreted as a form of increasing the stability of the classification, and thereby reducing uncertainty, which we hypothesize to be the key to better generalization.

#### 3.2. Datasets and Evaluation

We demonstrate the efficacy of our method on the standard domain adaptation tasks of GTA [58]→ Cityscapes [17] (GTA-CS) and Synthia [60]→ Cityscapes (SYN-CS) and Cityscapes→NTHU Crosscity [15] (CS-CC), a standard test setting used in several previous works (Section 4). Cityscapes consists 2975 annotated images, each of size \( 2048 \times 1024 \), that act as our training set. It has
500 images as the validation set, which we use to benchmark our method. It consists of 19 semantic classes for segmentation. The GTA dataset consists of 24966 frames, of size 1914 × 1052 grabbed from the famous game Grand Theft Auto. The ground truth is generated by the game renderer itself. It shares the same 19 semantic classes as Cityscapes. Synthia has 9400 images of size 1280 × 760 synthetic images, and shares 16 classes with Cityscapes. For our method, we use a network trained on Synthia or GTA, and adapt it to Cityscapes using the 2975 training images without their ground-truth labels. Crosscity dataset has been recorded in four cities: Rome, Rio, Taipe, and Tokyo with each image of resolution 2048 × 1024. Following [12], we use their experimental setup of 3200 unlabeled images as target training data, and 100 labeled images as target test data. This adaptation task has 13 shared classes. We use the pretrained models provided by Chen et al. [12] for the source trained model.

To evaluate our method, we use Intersection-over-Union (IoU) for each class, and its average mean-Intersection-over-Union (mIoU) over all classes. We report the metrics for all the 19 classes of GTA-CS adaptation, for the 16 common classes for the SYN-CS experiments, and for the 13 common classes in the CS-CC experiments. In accordance with some recent papers, we also report a mIoU∗ comparing only 13 classes for the Synthia to Cityscapes adaptation task.

3.3. Implementation details

To facilitate a fair comparison with relevant works, we use a DeepLab V2 network [10] with a ResNet-101 backbone [31]. Using the notation defined in Section 2, g is the ResNet-101 based feature extractor, and h is the Atrous Spatial Pyramidal Pooling (ASPP) decoder. The ResNet 101 backbone is pre-trained on ImageNet. ASPP [10] is a multi-scale decoder, that is used to aggregate multi-scale information for segmentation. It has 4 parallel atrous convolutions of various rates, which capture long-range contextual information from extracted features. We train the model on the source domain with stochastic gradient descent with a learning rate of 2.5 × 10−4 with a weight decay of 0.0005, momentum of 0.9. We use a poly learning rate decay scheduler with power of 0.9. For the adaptation experiments, we use a lower learning rate of 5 × 10−5, with other parameters staying the same, with no learning rate decay. We also use a 10× the learning rate for ASPP decoders [10] in our experiments. For all our experiments, we use λent = 1.0, λun = 0.1. We use the defaults prescribed by Zou et al. [80] to extract class-balanced pseudo labels. For the CS-CC experiments, we run the adaptation for only 2 epochs, and for GTA-CS, SYN-CS for 6 epochs. Code will be available at https://git.io/JthPp.

3.4. Results

We show the performance of our proposed method on the tasks of GTA-CS adaptation in Table 1a, SYN-CS adaptation in Table 1b and CS-CC adaptation in Table 1c. We obtain results that are at-par or better than some of the classic works on unsupervised domain adaptation (with source data). This work is, however, not a claim that source data is not necessary for domain adaptation. The utility of source data has been exploited effectively by recent methods through style transfer techniques [72, 35], thus they obtain higher performance than us. Our proposed method improves substantially on the larger background classes, and we hypothesize this is because the source classifier can make reliable predictions for these classes. The perceptual domain gap seems to influence the transfer performance too, as we get very comparable performance for GTA-CS and CS-CC experiments, compared to the results we obtain for SYN-CS experiments.
### (a) Results of GTA5 → Cityscapes (GTA-CS) domain adaptation.

| City       | Uses source data | Method       | Road     | Sidewalk   | Building  | Wall       | Fence     | Pole      | Tlx. light | Tlx. Sign | Veg.     | Sky       | Person    | Rider    | Car       | Truck     | Bus       | Team       | Motorcycle | Blue | mIoU  |
|------------|------------------|--------------|----------|------------|-----------|------------|-----------|----------|------------|-----------|----------|----------|----------|----------|----------|----------|----------|----------|------------|------------|-----|------|
| **Rome**   | Yes              | AdaptSegNet  | 86.5     | 36.0       | 79.9      | 23.4       | 23.3      | 23.9     | 14.8      | 83.4      | 33.3     | 75.6     | 58.5     | 27.6     | 73.7     | 32.5     | 35.4     | 3.9       | 30.1      | 28.1      | 42.4 |      |
|            |                  | AdvEnt [69]  | 89.4     | 33.1       | 81.0      | 26.6       | 26.8      | 27.2     | 33.5      | 24.7      | 83.9     | 36.7     | 78.8     | 30.5     | 84.8     | 38.5     | 44.5     | 1.7       | 31.6      | 32.4      | 45.5 |      |
|            |                  | FCAN [70]    | 91.2     | 33.1       | 81.0      | 26.6       | 26.8      | 27.2     | 33.5      | 24.7      | 83.9     | 36.7     | 78.8     | 30.5     | 84.8     | 38.5     | 44.5     | 1.7       | 31.6      | 32.4      | 45.5 |      |
|            |                  | CBST [81]    | 91.8     | 53.5       | 80.5      | 32.7       | 21.0      | 34.0     | 28.9      | 20.4      | 83.9     | 34.2     | 80.9     | 53.1     | 24.0     | 82.7     | 30.3     | 35.9     | 16.0      | 25.9      | 42.8      | 45.9 |      |
|            |                  | MRKLD [80]   | 91.0     | 55.4       | 80.0      | 33.7       | 21.4      | 37.3     | 32.9      | 24.5      | 85.0     | 34.1     | 80.8     | 57.7     | 24.6     | 84.1     | 27.8     | 30.1     | 26.9      | 26.0      | 42.3      | 47.1 |      |
|            |                  | LRENT [80]   | 91.8     | 53.5       | 80.5      | 32.7       | 21.0      | 34.0     | 29.0      | 20.3      | 83.9     | 34.2     | 80.9     | 53.1     | 23.9     | 82.7     | 30.2     | 35.6     | 16.3      | 25.9      | 42.8      | 45.9 |      |
|            | No               | Source       | 71.3     | 19.2       | 69.1      | 18.4       | 10.0      | 35.7     | 27.3      | 6.8       | 79.6     | 24.8     | 72.1     | 57.6     | 19.5     | 59.5     | 15.5     | 15.1     | 11.7      | 21.1      | 12.0      | 33.8 |      |
|            |                  | Our method   | 92.3     | 55.2       | 81.6      | 20.8       | 18.8      | 37.1     | 17.7     | 12.1      | 84.2     | 35.9     | 83.8     | 27.7     | 24.1     | 81.7     | 27.5     | 44.3     | 9.9       | 24.1      | 40.4      | 45.1 |      |

### (b) Results of Synthia → Cityscapes (SYN-CS) domain adaptation.

<table>
<thead>
<tr>
<th>City</th>
<th>Uses source data</th>
<th>Method</th>
<th>Road</th>
<th>Sidewalk</th>
<th>Building</th>
<th>Wall*</th>
<th>Pole*</th>
<th>Tlx. light</th>
<th>Tlx. Sign</th>
<th>Veg.</th>
<th>Sky</th>
<th>Person</th>
<th>Rider</th>
<th>Car</th>
<th>Truck</th>
<th>Bus</th>
<th>Team</th>
<th>Motorcycle</th>
<th>Blue</th>
<th>mIoU</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rome</strong></td>
<td>Yes</td>
<td>AdaptSegNet</td>
<td>84.3</td>
<td>42.7</td>
<td>77.5</td>
<td></td>
<td></td>
<td>4.7</td>
<td>7.0</td>
<td>77.9</td>
<td>82.5</td>
<td>54.3</td>
<td>21.0</td>
<td>72.3</td>
<td>32.2</td>
<td>18.9</td>
<td>32.3</td>
<td>46.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AdvEnt [69]</td>
<td>86.0</td>
<td>29.9</td>
<td>76.3</td>
<td>10.8</td>
<td>1.4</td>
<td>33.9</td>
<td>22.8</td>
<td>29.5</td>
<td>77.6</td>
<td>78.3</td>
<td>60.6</td>
<td>28.3</td>
<td>81.6</td>
<td>23.5</td>
<td>18.8</td>
<td>39.8</td>
<td>42.6</td>
<td>48.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CBST [81]</td>
<td>67.7</td>
<td>32.2</td>
<td>73.9</td>
<td>10.7</td>
<td>1.6</td>
<td>37.4</td>
<td>22.2</td>
<td>31.2</td>
<td>80.8</td>
<td>80.5</td>
<td>60.8</td>
<td>29.1</td>
<td>82.8</td>
<td>25.0</td>
<td>19.4</td>
<td>45.3</td>
<td>43.8</td>
<td>50.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MRKLD [80]</td>
<td>66.5</td>
<td>50.3</td>
<td>74.6</td>
<td>13.8</td>
<td>1.5</td>
<td>35.8</td>
<td>23.1</td>
<td>29.1</td>
<td>77.0</td>
<td>77.5</td>
<td>60.1</td>
<td>28.5</td>
<td>82.2</td>
<td>22.6</td>
<td>20.1</td>
<td>41.9</td>
<td>42.7</td>
<td>48.7</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Source</td>
<td>64.3</td>
<td>21.3</td>
<td>73.1</td>
<td>2.4</td>
<td>1.1</td>
<td>31.4</td>
<td>7.0</td>
<td>27.7</td>
<td>63.1</td>
<td>67.6</td>
<td>42.2</td>
<td>19.9</td>
<td>73.1</td>
<td>15.3</td>
<td>10.5</td>
<td>38.9</td>
<td>34.9</td>
<td>40.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Our method</td>
<td>59.3</td>
<td>24.6</td>
<td>77.0</td>
<td>14.0</td>
<td>1.8</td>
<td>31.5</td>
<td>18.3</td>
<td>32.0</td>
<td>83.1</td>
<td>80.4</td>
<td>46.3</td>
<td>17.8</td>
<td>76.7</td>
<td>17.0</td>
<td>18.5</td>
<td>34.6</td>
<td>39.6</td>
<td>45.0</td>
</tr>
</tbody>
</table>

### (c) Results of Cityscapes → Cross-City (CS-CC) experiments.

Table 1: For all the experiments in Tables 1a to 1c we compare our proposed method with methods that use source data for adaptation. We find that our method is comparable, and in some cases better than the methods that use the source data for adaptation. In underling, we compare our results to the source trained classifier, and with an bold the best performance over all methods. We omit the underline if our proposed method, or the source classifier out performs the method that use the source data for adaptation.

#### 3.4.1 Importance of loss terms

In order to correctly attribute performance to each of the terms in Equation (6), we ablate over the loss terms in Table 2. Broadly summarizing, we find that the first choice of using pseudo-labeling results in a substantial improvement of performance over the source classifier. With each term we see that the performance increases, however as described in Section 3.4.2, our method also suffers higher variance.
Deep learning had its success in semantic segmentation with fully convolutional networks [45], which converted the full-connected layers to convolutional layers. Following this, various networks that made several architectural changes to improve accuracy metrics [74, 79, 10], and computational requirements [78, 56, 59, 53] have been proposed. To remedy the data hungriness of these networks, domain adaptation, specifically unsupervised domain adaptation, has been an oft studied problem recently.

3.4.2 Variance analysis

In order to obtain a better estimate of performance, we run some of the baseline methods that we use in Table 1a with five random seeds and show the performance. We use the publicly available codes from the authors. For each method, we change only the random seed for each run, and leave the rest of the hyperparameters to the default values set by the authors in their codes. In Table 3, we show various statistics computed over the obtained runs. We see that the common trend in publications on UDA is to report the best obtained performance. While it is a pragmatic choice to use the best obtained model as benchmarked on a validation set, for deployments, it induces a systemic bias in the assessment of the true performance of the system. Thus, we believe that better characterization of the system’s performance is through computing the average performance and the standard deviation, in addition to the best performance obtained.

In Table 3, we find that merely changing the random seed can have a noticeable effect on the performance of some of the standard systems, an observation made before [48, 3]. The discrepancy between the maximum results in Table 3 and the reported numbers can be attributed to hardware and software discrepancies, or budget used. Vu et al. [69] also remark that one needs to run the experiments a few times to reach comparable performance. Keeping in line with the standards of the domain, we report the best obtained performance in Tables 1a to 1c, and show results of variance analysis in Tables 3 and 4. Examining the mean and standard deviation obtained for our GTA-CS and CS-CC experiments, we find that while our method achieves higher maximum performance, it has a higher variance compared to the previous loss values.

Thus, for a new use case one might expect a small but consistent improvement with pseudo-labeling, and other loss terms are useful if the method can be tuned carefully. We show various additional ablations in Appendix D, and some qualitative results in Appendix E.

### 4. Related Work

**Semantic Segmentation** Deep learning had its success in semantic segmentation with fully convolutional networks [45], which converted the full-connected layers to convolutional layers. Following this, various networks that made several architectural changes to improve accuracy metrics [74, 79, 10], and computational requirements [78, 56, 59, 53] have been proposed. To remedy the data hungriness of these networks, domain adaptation, specifically unsupervised domain adaptation, has been an oft studied problem recently.

**Unsupervised Domain Adaptation** Based on the seminal work of adversarial domain adaptation [26] that uses a discriminator network to align features from both domains, several methods have been proposed for segmentation on similar lines. Methods have been proposed that align intermediate feature spaces [33, 61, 22, 70], output space [66, 67].

Another family of methods use pseudo-labeling to enrich the target domain training using either hard labels [81, 18, 

---

**Table 2:** Importance of each of the loss terms proposed. \( \mathcal{L}_{DT} \) refers to training with loss in Equation (6) without freezing the decoders, and the last column \( \mathcal{L} \) shows the performance on freezing the main decoder. We see that each of the loss terms gives a consistent improvement over the previous loss values.

<table>
<thead>
<tr>
<th>Method</th>
<th>Performance estimate</th>
<th>Min</th>
<th>Reproduced Results</th>
<th>Previously Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdaptSegnet [66]</td>
<td>39.68 ± 1.49</td>
<td>37.70</td>
<td>42.20</td>
<td>42.40</td>
</tr>
<tr>
<td>ADVENT [69] (90K)</td>
<td>41.57 ± 0.73</td>
<td>40.73</td>
<td>42.73</td>
<td>43.80</td>
</tr>
<tr>
<td>ADVENT [69] (Best)</td>
<td>42.56 ± 0.64</td>
<td>41.60</td>
<td>42.39</td>
<td>42.39</td>
</tr>
<tr>
<td>CBST [81]</td>
<td>44.04 ± 0.88</td>
<td>42.80</td>
<td>45.03</td>
<td>45.90</td>
</tr>
<tr>
<td>Proposed Method</td>
<td>42.44 ± 2.18</td>
<td>39.71</td>
<td>45.06</td>
<td>–</td>
</tr>
</tbody>
</table>

**Table 3:** Variance of the methods examined for the GTA→Cityscapes. We show the mean, standard deviation, minimum and reproduced (maximum) performance obtained over five runs with different random seeds, and the official reported metrics from the paper. For ADVENT we show two rows to indicate the two testing strategies in their code: The first one is after 90K iterations, and the second is the best attained performance. We see that the common strategy is to report the best obtained result.

<table>
<thead>
<tr>
<th>Method</th>
<th>Performance estimate</th>
<th>Min</th>
<th>Reproduced Results</th>
<th>Previously Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rome</td>
<td>53.2 ± 0.8</td>
<td>52.37 ± 1.08</td>
<td>49.2 ± 0.71</td>
<td>49.48 ± 0.76</td>
</tr>
<tr>
<td>Rio</td>
<td>53.2 ± 0.8</td>
<td>52.37 ± 1.08</td>
<td>49.2 ± 0.71</td>
<td>49.48 ± 0.76</td>
</tr>
<tr>
<td>Tokyo</td>
<td>53.2 ± 0.8</td>
<td>52.37 ± 1.08</td>
<td>49.2 ± 0.71</td>
<td>49.48 ± 0.76</td>
</tr>
<tr>
<td>Taipei</td>
<td>53.2 ± 0.8</td>
<td>52.37 ± 1.08</td>
<td>49.2 ± 0.71</td>
<td>49.48 ± 0.76</td>
</tr>
</tbody>
</table>

**Table 4:** Variance of proposed method for the Cityscapes→NTHU Crosscity adaptation.

---

[1] https://github.com/valeoai/ADVENT#training
or soft labels [80]. Chang et al. [5] use a per-domain autoencoder to separate domain idiosyncrasies from features relevant for cross-domain segmentation. Vu et al. [69], Chen et al. [12] propose an entropy based objective, and an adversarial alignment of the entropy maps of the two domains.

A host of techniques include style translation as a part of their network that is trained along with the segmentation network [32, 43, 14, 50], or separately [72, 35].

**Model Adaptation** Most of the previously mentioned methods need the explicit availability of source domain data during adaptation too, and have made tremendous strides in improving the segmentation performance in that case. A few recent papers tackle model adaptation for classification problems [44, 42, 16]. [39] proposes source-free domain adaptation in the case where label knowledge of the target domain is not available, and show their efficiency on a set of classification problems with varying levels of label overlap. As we argued in Section 1, to the best of our knowledge, this problem has not been tackled in the context of semantic segmentation. Though the task of segmentation can be construed to be one that of pixel-wise prediction, we emphasize that the techniques cannot be interchangeably used. As the resource requirements of segmentation networks are substantially higher than that of classification networks, methods proposed classification that use label conditioned generation [42] of target domain data, or use memory intensive methods for reliable estimation of pseudo-labels [36, 44] are impractical.

**Self-supervision for segmentation** Self-supervised learning exploits the structure in data by defining a pretext task, so that the network learns a good semantic representation of the input image. Examples include rotation prediction [27], context prediction [21], jigsaw puzzle solving [52], contrastive learning [13, 30]. Self-supervised learning for unsupervised domain adaptation has been proposed to train the feature extractor [64]. However, the applications of self-supervised learning to segmentation have been limited, as the invariances enforced differ widely between classification and segmentation problems. Some attempts to learn segmentation networks include using very strong perturbation techniques like CutMix [24], using consistency regularization through feature noising [54], by using clustering for pseudo-labels [40]. As described in Section 2.2, we note similarities of our method to tasks proposed in [54].

**Multi-task learning and robust classification** The use of multiple tasks to enrich the representations learned by a network has been used quite often in computer vision [77, 4]. These ideas have been adapted to single task learning by devising pseudo-tasks [49]. These pseudo-tasks train the shared network structure to learn the task in multiple ways, and can be interpreted as using self-supervision. Similarly, increasing the robustness of classification through feature noising has been studied extensively [28, 8, 68, 16, 47]. Work on learning robust networks through pseudo-ensambling by reducing the variance when dropout is used, has been proposed [2]. Ideas of large margin learning have been extended to deep learning [23].

**Uncertainty modeling for neural networks** Our proposed method in Section 2.2 is very similar to the uncertainty modeling for neural networks using Monte-Carlo (MC) dropout. MC-dropout [34, 25] uses dropout at test-time to sample various outputs and average them for predicted posterior. Bayesian treatments of neural networks have been important owing to their ability to predict uncertainty better, and dealing with mis-calibration problems [38]. Such modeling has been used for medical imaging to estimate the confidence of lesion segmentation [51], for autonomous driving to estimate the uncertainty of steering wheel angle prediction [46].

5. Conclusion

In this paper, we focus on the problem of domain adaptation for semantic segmentation in the absence of source data. In the absence of any labels to guide the optimization, we propose a method that reduces the uncertainty of predictions on the target domain data, that can also be interpreted as increasing the stability of the feature extractor. On the standard benchmark of tasks for semantic segmentation transfer, we obtain performance comparable with that of methods that use source data. We hope that our work gives the required fillip to the community to focus on this newer, practically significant, and challenging form of domain adaptation.

Acknowledgments

The research leading to these results was supported by the “Swiss Center for Drones and Robotics - SCDR” of the Department of Defence, Civil Protection and Sport via armasuisse S+T under project n°050-38.

References


[34] Alex Kendall and Yarin Gal. What uncertainties do we need in bayesian deep learning for computer vision? In Advances in neural information processing systems, pages 5574–5584, 2017. 8
[44] Jian Liang, Dapeng Hu, and Jiashi Feng. Do we really need to access the source data? source hypothesis transfer for unsupervised domain adaptation. In International Conference on Machine Learning (ICML), pages xx–xx, July 2020. 4, 8
09–15 Jun 2019. PMLR. 1


[63] Daniel L Silver, Qiang Yang, and Lianghao Li. Lifelong machine learning systems: Beyond learning algorithms. In 2013 AAAI spring symposium series, 2013. 1


Uncertainty Reduction for Model Adaptation in Semantic Segmentation

Appendix

Prabhu Teja S
Idiap Research Institute & EPFL
prabhu.teja@idiap.ch

François Fleuret
University of Geneva & Idiap Research Institute
francois.fleuret@unige.ch

A. Toy example’s network architecture

For the toy experiment presented in Section 3.1, we use a network from Kristiadi et al. [38]. The architectural details of the network are given in Table 5.

Table 5: Architecture of the network used for the toy experiment in Figure 3

<table>
<thead>
<tr>
<th>Layer name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Extractor</td>
<td><a href="2">Linear 2 × 20</a></td>
</tr>
<tr>
<td></td>
<td>BatchNorm</td>
</tr>
<tr>
<td></td>
<td>ReLU</td>
</tr>
<tr>
<td></td>
<td>Linear 20 × 2</td>
</tr>
<tr>
<td></td>
<td>ReLU</td>
</tr>
<tr>
<td>Classifier</td>
<td>Softmax(2)</td>
</tr>
</tbody>
</table>

B. Entropy measurements

In Figure 1 and in Section 2.1, we glossed over the details of the toy-problem. We provide the details here.

Referring to Figure 1, we are trying to reason scenarios that, in the absence of labeled target data, can be expected to result in good target performance. Our argument is that reducing the uncertainty of predictions on the target domain is an effective strategy to improve performance on the target domain. In order to do so, we concoct toy scenarios, and analyse their uncertainties. For this illustration, we use entropy as a measure of the uncertainty.

Let us consider a two-class classification problem as shown in Figure 1. Let \( X \) be the feature random variable, and \( Y \in \{0, 1\} \) be the labels. Let us assume that the class conditional distributions be normally distributed i.e. \( X|Y = k \sim \mathcal{N}(\mu_k, \sigma^2) \). Thus \( \mu_X(x) = \frac{1}{2} \left( \mathcal{N}(x; \mu_0, \sigma^2) + \mathcal{N}(x; \mu_1, \sigma^2) \right) \), assuming uniform prior on \( Y \). Let the threshold random variable \( T \) with a density \( \mu_T(t) \). This distribution is determined by a learning algorithm. Let \( \hat{Y} \) be the random variable denoting the predictions whose probability is computed using a sigmoid on the feature and a threshold as

\[
\rho(x; t) \equiv p(\hat{Y} = 1|X = x; T = t) = \frac{1}{1 + e^{-(x-t)}}. \tag{7}
\]

The entropy of the above defined categorical distribution is given by

\[
\mathbb{H}(\hat{Y}|X = x, T = t) = - (\rho(x; t) \log(\rho(x; t)) + (1 - \rho(x; t)) \log(1 - \rho(x; t))) \tag{8}
\]

The entropy of a classification over the entire domain \( X \) can be computed as

\[
\mathbb{H}(\hat{Y}|T = t) = \int - (\rho(x; t) \log(\rho(x; t)) + (1 - \rho(x; t)) \log(1 - \rho(x; t))) \mu_X(x) dx \tag{9}
\]
The above defined marginal entropy is defined for a specific choice of the threshold $t$. To see the how the feature distribution itself influences the generalization, the entropy over all possible thresholds is computed. The total entropy over all the thresholds possible is computed by integrating over the entire range of $t$.

$$H(\hat{Y}) = \int \int - (\rho(x; t) \log(\rho(x; t)) + (1 - \rho(x; t)) \log(1 - \rho(x; t))) \mu_X(x)\mu_T(t)dxdt$$  \hspace{1cm} (10)$$

We emphasize that $t$ is the set of thresholds that can be generated by a learning algorithm. However, we simplify it to using the domain $X$ for this discussion.

We would like to train networks that result in low overall entropy in Equation (10). This coincides with out argument that the features that can be separated by several choices of threshold are likelier to generalize better. To visualize this, we run a few simulations that compute the marginal and total entropy for various settings of feature distributions. In Figure 4, we show the data distribution $\mu_X(x)$ for various $\mu_0, \mu_1$ values. Variance $\sigma^2$ is fixed to 1. In orange, we show marginalized entropy (Equation (9)). We scale it by a constant for plotting purposes.

It is very apparent that the higher is $|\mu_1 - \mu_2|$, lower the overall entropy. Given that the two Gaussians are the class conditional distributions, the Bayes optimal decision boundary, that can be computed to be $\frac{\mu_1 + \mu_2}{2}$, coincides with the point where Equation (9) is minimized, for all scenarios except for the one with high overlap in Figure 4(a). Extending it, the lower is the Bayes risk, better is the generalization. Thus the least entropy separation is also the best separator we can achieve. We skip an important detail here: by extending the threshold search to a value that is on the extremities of the $X$-axis, we can get a threshold that results in an overall entropy that is very low. However, such a separator is practically useless. In our method, we avoid this by using the pseudo-labeling and the initializing the network with the source trained weights.

We can see that for this simple scenario that minimizing the entropy is a fairly good strategy in the absence of labels to find near optimal decision boundary.
C. Using squared error instead of entropy loss in Equation (2)

In Section 2.2, we proposed the uncertainty loss, and we use a squared error form instead of the standard entropy based uncertainty quantification. Here we provide a plausible explanation that follows the argument in Chen et al. [12]. Experimental evidence is provided in [54].

The traditional entropy regularizer has been used extensively in various applications like semi-supervised learning [29], domain adaptation [69]. However, the gradient of the entropy penalty with respect to the softmax output is not well behaved for probability is close to 1. We refer the reader to [12, Figure 1] for an illustration of this. However, squared loss and entropy loss can be viewed as a special case of $f$-divergence.

Let $P$ and $Q$ be two distributions with pdfs $p$ and $q$ their density functions. Then their $f$-divergence is defined as

$$D_f(P||Q) = \int_{\mathbb{R}} f\left(\frac{p(x)}{q(x)}\right) q(x) dx$$ \hspace{1cm} (11)

We get KL-divergence by using $f(t) = t \log t$. Instead, using $f(t) = (t - 1)^2$ gives the Max-squared loss formulation in [12]. They find that using this instead of $f(t) = t \log t$ results in better behavior for optimization. We find a similar empirical result that using the squared error form for Equation (2) results in better results than using posterior entropy.

D. Experimental ablations

D.1. Sensitivity to auxiliary decoders

In the numbers reported in Tables 1a and 1b, we use a dropout ratio of $p = 0.5$. We show an ablation on the dropout values in Table 6. Intuitively, this value indicates the level of noise resiliency that we expect in the network; a too low a value has very little use as it is equivalent to having a single decoder without dropout, and too high a value destroys too much information fed to the decoders. Thus an intermediate value like 0.5 is likely to be more appropriate for our use. We find that our experiments support this notion in Table 6. For this comparison, we use 5 auxiliary decoders. However, our proposed method is quite robust to this choice.

<table>
<thead>
<tr>
<th>Dropout (p)</th>
<th>0.2</th>
<th>0.5</th>
<th>0.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance (mIoU) %</td>
<td>44.44</td>
<td>45.07</td>
<td>44.14</td>
</tr>
</tbody>
</table>

Table 6: Optimal feature dropout proportions for GTA $\rightarrow$ Cityscapes experiment.

D.2. Number of auxiliary decoders

The auxiliary decoders play an important role in the level of feature stability induced. Indeed Gal and Ghahramani [25] show that larger the number of samples drawn from the dropout distribution, better is the approximation. In Table 7, we see that the number of decoders plays an important role, but the method is fairly stable in its performance over a range of decoder count.

<table>
<thead>
<tr>
<th># Decoders</th>
<th>1</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance (mIoU)</td>
<td>43.5</td>
<td>44.20</td>
<td>44.67</td>
<td>45.07</td>
</tr>
</tbody>
</table>

Table 7: Performance variation to the number of auxiliary decoders for GTA $\rightarrow$ Cityscapes experiment.

D.3. Using single dropout decoder

In our method we propose the use of multiple decoders instead of one, and we show the effect of using a single decoder to decode the noisy features in Table 8. While it conceptually seems that using a single decoder should suffice, we see that using multiple auxiliary decoders is helpful. Using multiple decoders forces the feature extractor to be more robust, whereas using a single decoder forces the decoder to be more stable. However, the ASPP decoder is one layer deep, its representation capacity is limited and thus it is unable to do so, as evidenced in Table 8.
<table>
<thead>
<tr>
<th>Method</th>
<th>mIoU %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single decoder with dropout</td>
<td>43.29</td>
</tr>
<tr>
<td>Multiple auxiliary decoders</td>
<td>45.07</td>
</tr>
</tbody>
</table>

Table 8: Utility of using multiple decoders

E. Qualitative results for Cityscapes to Cross City Adaptation

In Figures 5 to 8 we show some qualitative improvements from our results for the CS-CC experiments.

Figure 5: Best five case results of adaptation for the Cityscapes to Rome (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 6: Best five results of adaptation for the Cityscapes to Rio (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 7: Best five results of adaptation for the Cityscapes to Taipei (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 8: Best five results of adaptation for the Cityscapes to Tokyo (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.

E.1. Failure cases

In Figures 9 to 12, we show the five images that have least improved over the adaptation process.
Figure 9: Worst five results of adaptation for the Cityscapes to Rome (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 10: Worst five results adaptation for the Cityscapes to Rio (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 11: Worst five results adaptation for the Cityscapes to Taipei (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.
Figure 12: Worst five results adaptation for the Cityscapes to Tokyo (Cross City). The first column is the test image, the second column is the ground truth, the third and fourth columns are the source trained model, and results of our proposed method.