Active Learning by Feature Mixing
(Supplements)

Amin Parvaneh1  Ehsan Abbasnejad1  Damien Teney1,2  Reza Haffari3,
Anton van den Hengel1,4  Javen Qinfeng Shi1

1Australian Institute for Machine Learning, University of Adelaide
2Idiap Research Institute  3Monash University  4Amazon
{amin.parvaneh, ehsan.abbasnejad, javen.shi, anton.vandenhengel}@adelaide.edu.au
damien.teney@idiap.ch  gholamreza.haffari@monash.edu

1. Methodology

Details of Eq. (2) in the main text. We can write the first-order Taylor expansion of the
loss for an interpolation w.r.t. \(z^u\) as:
\[
\ell(f_c(\tilde{z}_\alpha), y^*) \approx \ell(f_c(z^u), y^*) + (\tilde{z}_\alpha - z^u)^\top \nabla_{z^u}\ell(f_c(z^u), y^*),
\]
(1)
\[
\text{We also know that considering } \tilde{z}_\alpha = \alpha z^* + (1 - \alpha) z^u, \text{ we will have}
\]
\[
\tilde{z}_\alpha - z^u = (\alpha z^* + (1 - \alpha) z^u) - z^u
\]
\[
= \alpha z^* + z^u - \alpha z^u - z^u
\]
\[
= \alpha z^* - z^u
\]
\[
= \alpha(z^* - z^u). \tag{2}
\]
By replacing this in Eq. (1), we have
\[
\ell(f_c(\tilde{z}_\alpha), y^*) \approx \ell(f_c(z^u), y^*) + (\alpha(z^* - z^u))^\top \nabla_{z^u}\ell(f_c(z^u), y^*). \tag{3}
\]
which uncovers Eq. (2) in the main text.

Details of Eq. (5) in the main text. As stated in section 3.3 of the main text, using a 2-norm constraint on \(\alpha\), we approximate the optimum interpolation ratio as
\[
\alpha^* = \arg \max_{\|\alpha\|_2 \leq \epsilon} (\alpha(z^* - z^u))^\top \nabla_{z^u}\ell(f_c(z^u), y^*). \tag{4}
\]
By multiplying both sides of the constraint in Eq. 4 by \(\|z^* - z^u\|_2\), we have
\[
\|\alpha\|_2 \|z^* - z^u\|_2 \leq \epsilon \|z^* - z^u\|_2.
\]
Based on Cauchy-Schwartz inequality, we know that
\[
\|\alpha(z^* - z^u)\|_2 \leq \|\alpha\|_2 \|z^* - z^u\|_2.
\]
Thus, we can infer
\[
\|\alpha(z^* - z^u)\|_2 \leq \epsilon \|z^* - z^u\|_2 = \epsilon.
\]
Therefore, we can change the optimisation problem to
\[
\alpha^* = \arg \max_{\|\alpha\|_2 \leq \epsilon} (\alpha(z^* - z^u))^\top \nabla_{z^u}\ell(f_c(z^u), y^*).
\]
We can use the dual norm \([3]\) of the above equation to approximate the optimum value for \(u = \alpha(z^* - z^u)\), which is
\[
u^* = \epsilon \frac{\nabla_{z^u}\ell(f_c(z^u), y^*)}{\|\nabla_{z^u}\ell(f_c(z^u), y^*)\|_2} \tag{5}
\]
After replacing the actual values for \(u\) and \(\epsilon\), we have
\[
\alpha^* \approx \epsilon \frac{\|z^* - z^u\|_2 \nabla_{z^u}\ell(f_c(z^u), y^*)}{\|\nabla_{z^u}\ell(f_c(z^u), y^*)\|_2} \odot (z^* - z^u), \tag{6}
\]
which reveals Eq. (5) in the main text (\(\odot\) indicates element-wise division).

It is worth mentioning that the denominator in Eq. 6 cancels out when utilised for the interpolation and as such does not present any divide by zero problem in our approach. Consider that we use \(\alpha^*\) in the following:
\[
\tilde{z}_{\alpha^*} = \alpha^* z^* + (1 - \alpha^*) z^u
\]
\[
= z^u + \alpha^*(z^* - z^u), \tag{7}
\]
where its value is obtained from the closed-form solution in Eq. 6. When considering both together, it is easy to see that the denominator simply cancels out with \((z^* - z^u)\). In practice, adding a very small constant to the denominator provides numerical stability and resolves this issue.

1.1. Relations Between ALFA-Mix and Other Baselines

Using gradients in BADGE: From Eq. (3) in the main text we can understand that when the prediction is accurate and
confident, small movements of the latent representation towards different directions (declared by anchors) should not change the prediction. Otherwise, as per right-hand-side of the equation, either the surface has changed dramatically or the unlabelled features is far from the labelled representations (i.e., the features of the unlabelled instance are novel). This is one of the major differences of our approach when compared with BADGE that only relies on the gradients of the unlabelled instances (Figure 1).

Adversarial perturbation of features: To show the importance of the feature interpolations with labelled representations in our approach, we also considered using adversarial noise as an alternative perturbation mechanism. For that, we examined adding small values of noise $\delta$ to the latent representations of each unlabelled point (instead of using interpolations with anchors) to find inconsistencies in their predicted labels. Following Eq. (3) and Eq. (4) in the main text, we set the objective for finding the optimum noise vector $\delta^*$ as:

$$\delta^* = \arg \max_{\|\delta\| \leq \epsilon} \ell(f_c(z^u + \delta), y^u).$$  \hspace{1cm} (8)

Similarly, using a first-order Taylor expansion w.r.t. $z^u$ and its dual norm, we can approximate the optimum noise as

$$\delta^* \approx \epsilon \frac{\nabla_{z^u} \ell(f_c(z^u), y^u)}{\|\nabla_{z^u} \ell(f_c(z^u), y^u)\|_2}.$$  \hspace{1cm} (9)

After constructing a candidate set of unlabelled samples whose predicted labels are not consistent after the adversarial feature perturbation, we conduct clustering to sample a diverse set from the candidate set (similar to ALFA-Mix).

Interestingly, as depicted in Figure 1b, although the adversarial approach shows better performance in comparison to BADGE, it falls behind considerably when compared to ALFA-Mix. We believe that the main advantage of ALFA-Mix is the consideration of both the novelty of the features and the extent of gradient at each unlabelled point. It is worth mentioning that ALFA-Mix is able to identify more inconsistencies all over the decision boundary (Figure. 6c in the main text).

Distribution matching. Denote $\Delta = \mathbb{E}_{p(z^1|\mathcal{D}^+)}[z^1] - \mathbb{E}_{p(z^u|\mathcal{D}^u)}[z^u]$ if we had the distributions in the latent space. We know that based on the definition of the interpolation between a pair of labelled and unlabelled samples (i.e., $\tilde{z}_\alpha = \alpha z^1 + (1 - \alpha) z^u$), we can have

$$z^u = \frac{1}{1 - \alpha} \left( \tilde{z}_\alpha - \alpha z^1 \right).$$

By taking the expectation from both side of the above equation for all the labelled samples we have

$$z^u = \mathbb{E}_{p(z^1|\mathcal{D}^+)} \left[ \frac{1}{1 - \alpha} \left( \tilde{z}_\alpha - \alpha z^1 \right) \right].$$

After replacing this in the definition of $\Delta$, it is easy to show that:

$$\Delta = \frac{1}{(1 - \alpha)} \left( \mathbb{E}_{p(z^1|\mathcal{D}^+)}[z^1] - \mathbb{E}_{p(z^u|\mathcal{D}^u)} \left[ \mathbb{E}_{p(z^1|\mathcal{D}^+)}[\tilde{z}_\alpha] \right] \right).$$

That is, the interpolation operation we used here only affects difference of the expectation of distributions with a constant factor. When seen in light of Eq. (1) in the main text, it acts as a simple surrogate for a divergence measure. In fact, this
“Continue” represents the setting where the weights of the network initialise from those of the network trained in the previous round.

These are two small subsets of DomainNet-Real that has been used to compare AL methods on small datasets with high-resolution images.

Table 1. A summary of diverse AL settings that we used in our image and non-image experiments. Overall, 30 different settings were utilised in our experiments to compare AL methods in various conditions.

* These are two small subsets of DomainNet-Real that has been used to compare AL methods on small datasets with high-resolution images.

**"Continue" represents the setting where the weights of the network initialise from those of the network trained in the previous round.

Gradient-based interpolation optimisation. Following [1, 10], we could have utilised iterative gradient-based optimisation to find the optimum interpolation ratios (instead of the closed-form solution used in ALFA-Mix). For that, motivated by the condition in the Eq. (6) in the main text where we are interested in instances whose predictions flip with an interpolation in the latent space, we can choose \( \alpha \) as a solution to the following:

\[
\alpha^* = \arg \max_{\alpha \in [0, \alpha_{\text{max}}]^D} \ell(f_c(\alpha z^* + (1 - \alpha) z^u), y^*), \tag{10}
\]

\[
\text{s.t. } y^* = \arg \max_{k \in \{1, \ldots, K\}} f^k_c(z^u), \quad \forall z^u \in Z^u, \quad z^* \in Z^*,
\]

where \( \alpha_{\text{max}} \) is a hyper-parameter governing the feature mixing ratios. Intuitively, this optimisation chooses the hardest case of \( \alpha \) for each unlabelled instance and anchor. We perform few iterations of projected gradient descent to optimise \( \alpha \). Our empirical studies reveal similar performances when using this objective in comparison to the closed-form one. However, the time required for the iterative gradient-based approach is much more than the closed-form one (i.e., when using 5 iterations of gradient update, it is 5x slower than ALFA-Mix).

2. Experiments

2.1. Comparison matrix

We demonstrate the performance comparison between every pair of AL methods over various settings in a penalty matrix proposed in [2]. Each cell of the matrix reveals the number of settings in which the method shown in the column is outperformed by the ones indicated in the row. It should be noted that each setting consists of conducting \( R \) rounds of AL with a specific labelling budget size \( B \) and using a particular model architecture on a single dataset. Since we repeat each setting with 5 different random seeds, at each round \( r \) in the setting we use \( t \)-score of the difference between the test performances \( (d_{i,j}^r = a^r_i - a^r_j) \) of each pair of AL methods \((i, j)\) over the 5 repeats:

\[
c_{i,j}^r = \frac{\sqrt{\mu^r}}{\sigma^r}, \tag{11}
\]

\[
\mu^r = \frac{1}{5} \sum_{m=1}^{5} d_{i,j}^r, \quad \sigma^r = \sqrt{\frac{1}{5} \sum_{m=1}^{5} (d_{i,j}^r - \mu^r)^2},
\]
where $a_i^r$ and $a_j^r$ are the test performances of methods $i$ and $j$ respectively at AL round $r$. Similar to [2], we also used a threshold of 2.776 for this score to decide if method $i$ wins over method $j$. After clarifying the winner at each round of the setting, we calculate $C_{i,j} = \sum_{r=1}^{R} \mathbb{1}_{r, i, j > 2.776} / R$ as the final victory score of AL method $i$ over method $j$ in that specific setting. Additionally, to compute the matrix over multiple settings, we simply report the element-wise sum of all the individual matrices.

### 2.2. Sampling Diversity and Uncertainty

To have a better understanding with regards to the effectiveness of our approach in selecting an uncertain and diverse set of samples for labelling, we compare some characteristics of the selected batch of instances at each AL round comparing our method with those from BADGE [2] and Margin-Based Sampling¹ [12] (Figure 3).

Comparing the confidence and Top-2 prediction margins of the selected unlabelled samples, depicted in Figures 3a and 3b respectively, we can see that the uncertainty level of the selected samples by our method is closer to the highest possible value in comparison to BADGE sampling. Please note that in contrast to what Margin-Based Sampling is doing, we do not explicitly enforce our approach to select samples close to the decision boundaries. On the other hand,

¹Margin-Based Sampling is another AL method based on uncertainty. It selects samples with the lowest distance between the predicted probabilities for the Top-2 classes (called margin). It should be noted that BADGE has shown significantly better performance compared to Margin-Based Sampling in prior works [2].
Figure 4. The t-SNE visualisation of the sample selection of our proposed method on MNIST dataset using LeNet-5. The model is trained based on 500 random labelled set (shown as triangles) and is provided with a budget of size 500 to (depicted as bold circles).

<table>
<thead>
<tr>
<th>Method</th>
<th>Random</th>
<th>Entropy</th>
<th>BALD</th>
<th>CoreSet</th>
<th>GCNAL</th>
<th>CDAL</th>
<th>BADGE</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>0.0</td>
<td>2.0</td>
<td>0.0</td>
<td>0.3</td>
<td>2.0</td>
<td>0.8</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Entropy</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>BALD</td>
<td>0.9</td>
<td>2.0</td>
<td>0.0</td>
<td>1.0</td>
<td>2.0</td>
<td>0.9</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CoreSet</td>
<td>0.1</td>
<td>1.9</td>
<td>0.0</td>
<td>0.0</td>
<td>1.6</td>
<td>0.8</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>GCNAL</td>
<td>0.0</td>
<td>1.9</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.5</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>CDAL</td>
<td>0.7</td>
<td>1.4</td>
<td>0.8</td>
<td>1.0</td>
<td>0.9</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>BADGE</td>
<td>1.4</td>
<td>2.0</td>
<td>1.1</td>
<td>1.8</td>
<td>2.0</td>
<td>1.1</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Ours</td>
<td>1.9</td>
<td>2.0</td>
<td>1.8</td>
<td>2.0</td>
<td>2.0</td>
<td>1.6</td>
<td>1.1</td>
<td>0.0</td>
</tr>
</tbody>
</table>

(a) Image (maximum value: 28)

(b) OpenML (maximum value: 2)

Figure 5. Pairwise comparison of different AL approaches based on the type of data. The maximum value of each cell for each setting is also provided in the captions.

considering the higher entropy values in the ground-truth labels of the selected set and their Top-2 predicted classes, we can realise the capability of our proposed method in selecting a diverse set of unlabelled samples in terms of their true class labels and their position with regard to the decision boundaries. All in all, as depicted in Fig. 4, our method is able to exploit both uncertainty and diversity concepts to select a diverse set of samples that lie close to decision boundaries, which leads to significantly higher performances.

2.3. More Ablations

In addition to providing the percentage with which our approach outperforms others in each setting (Table. 2), we report the pairwise comparison of all the AL methods across various choices of data (Fig. 5), budget size (Fig. 6), model architecture (Fig. 7) and network initialisation method (Fig. 8). Further, in Figure 6c, we provide the pairwise comparisons in low-data regimes. Considering the values in the rows and columns corresponding to our approach, we can
infer that our approach consistently outperforms all other baselines regardless of the architecture, dataset selection, network initialisation and budget size and is rarely beaten by others.

### 2.4. All the Experiments

We compare our approach with other baselines over a total of 285 AL rounds in 30 different settings, with each setting identified by a specific combination of dataset, budget size, model architecture, and model initialisation method. Table 2 demonstrates details of each setting we employed in our experiments.

In our approach, we set $\epsilon = \frac{0.2}{\sqrt{D}}$, where $D$ is the dimensionality of $\alpha$ vector. Considering the norm condition in Eq. 4 in the main text, we relate the scale of $\epsilon$ to $D$ to easily utilise the same hyper-parameter across different networks with representations of variable dimensions.

All the experiments for small datasets were carried out on a NVIDIA GeForce GTX 1080 Ti, while for larger datasets we used an NVIDIA QUADRO RTX 8000. It is worth mentioning that for the video experiments, we utilised two NVIDIA V100 GPUs in parallel.

We borrowed the implementations of the baselines from their publicly provided codes. The MLP network we employed in our experiments follows the architecture proposed in [2]: a two-layer Perceptron with ReLU activations and an embedding dimension of size 256 for image datasets (i.e. MNIST and EMNIST). Similarly, we expanded the embedding dimensionality to 1024 for OpenML datasets. We include the accuracy curves over the unseen test set for all the settings.

![Figure 6](image-url)  
Figure 6. Pairwise comparison of different AL approaches based on different sizes of budget. The maximum value of each cell for each setting is also provided in the captions.
Figure 7. Pairwise comparison of different AL approaches based on different model architectures. The maximum value of each cell for each setting is also provided in the captions.
Figure 8. Pairwise comparison of different AL approaches based on different sizes of budget. The maximum value of each cell for each setting is also provided in the captions.
Figure 9. Small Budget, ViT-Base, DomainNet-Real

Figure 10. Small Budget, ViT-Small, Mini-ImageNet

Figure 11. Small Budget, ViT-Small, CIFAR100

Figure 12. Small Budget, MLP, MNIST

Figure 13. Small Budget, MLP, MNIST, Continue

Figure 14. Small Budget, MLP, EMNIST
Figure 15. Small Budget, MLP, EMNIST, Continue

Figure 16. Small Budget, LeNet-5, MNIST

Figure 17. Small Budget, LeNet-5, MNIST, Continue

Figure 18. Small Budget, LeNet-5, EMNIST

Figure 19. Small Budget-ResNet-18, SVHN

Figure 20. Small Budget, ResNet-18, CIFAR10
Figure 21. Small Budget, ResNet-18, DomainNet-Real

Figure 22. Small Budget, ResNet-18, DomainNet-Real-10

Figure 23. Small Budget, ResNet-18, DomainNet-Real-20

Figure 24. Small Budget, DenseNet-121, SVHN

Figure 25. Small Budget, DenseNet-121, CIFAR10

Figure 26. Small Budget, DenseNet-121, DomainNet-Real
Figure 33. Large Budget, ResNet-18, SVHN

Figure 34. Large Budget, ResNet-18, CIFAR10

Figure 35. Large Budget, DenseNet-121, SVHN

Figure 36. Large Budget, DenseNet-121, CIFAR10

Figure 37. Small Budget, MLP, OpenML-6

Figure 38. Small Budget, MLP, OpenML-155
References


