ROBUST HYPERSPHERE-BASED WEIGHT IMPRINTING FOR FEW-SHOT LEARNING

Nikolaos Passalis\textsuperscript{1}, Alexandros Iosifidis\textsuperscript{2}, Moncef Gabbouj\textsuperscript{3} and Anastasios Tefas\textsuperscript{1}
\textsuperscript{1}\text{Department of Informatics, Aristotle University of Thessaloniki, Thessaloniki, Greece}
\textsuperscript{2}\text{Department of Engineering, Electrical and Computer Engineering, Aarhus University, Denmark}
\textsuperscript{3}\text{Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland}
E-mails: passalis@csd.auth.gr, ai@eng.au.dk, moncef.gabbouj@tuni.fi, tefas@csd.auth.gr

Abstract—Performing fast few-shot learning is increasingly important in a number of embedded applications. Among them, a form of gradient-descent free learning known as Weight Imprinting was recently established as an efficient way to perform few-shot learning on Deep Learning (DL) accelerators that do no support back-propagation, such as Edge Tensor Processing Units (Edge TPUs). Despite its efficiency, WI comes with a number of critical limitations. For example, WI cannot effectively handle multimodal novel categories, while it is especially prone to overfitting that can have devastating effects on the accuracy of the models on novel categorizes. To overcome these limitations, in this paper we propose a robust hypersphere-based WI approach that allows for regularizing the training process in an imprinting-aware way. At the same time, the proposed formulation provides a natural way to handle multimodal novel categories. Indeed, as demonstrated through the conducted experiments, the proposed method leads to significant improvements over the baseline WI approach.

Index Terms—Weight Imprinting, Few-shot Learning, Edge TPU, Embedded Deep Learning

I. INTRODUCTION

Deep Learning (DL) has achieved remarkable results on a wide range of especially challenging problems [1], which span from image understanding and visual questioning answering problems [2], to natural language processing [3], and video analysis [4]. Despite the success of DL on the aforementioned areas, DL models require powerful hardware both during the training process, as well as during the inference. The development of advanced Graphics Processing Units (GPUs) [5], as well as Tensor Processing Units (TPUs) [6], allowed for accelerating both the training and inference processes, as well as lowering the energy requirements of DL. However, most of these accelerators remain too bulky for many embedded applications, including robotics [7] and Internet-of-Things (IoT) applications [8], leading to developing extremely energy efficient hardware for accelerating only the inference process, such as Edge TPUs [9]. These platforms can lead to tremendous improvements in terms of operations/Watt. However, being designed to support inference-only operations, they are unable to support back-propagation, rendering impossible to perform on-device training. These limitations severely restrict their applications on open-word settings, which frequently occur in many applications, e.g., robotics [10], where DL models should be able to promptly adapt to emerging categories that were not seen during the training. This problem is known as few-shot learning or low-shot learning [11], [12], [13], where models are required to learn new categories and generalize the already encoded knowledge using just a few labeled examples.

Despite the large number of few-shot learning methods proposed in the literature [11], [12], [13], [14], just a few of them support inference-only DL accelerators. Perhaps the most widely known is the Weight Imprinting (WI) approach [15], which was recently proposed as the default way to perform training on the Google’s Edge TPU accelerator. WI allows for extending the classes a DL model can recognize by performing gradient descent-free learning. To this end, an appropriate vector prototype is calculated for each novel class and, then, this prototype vector is imprinted in the last classification layer of a DL model. Note that this process does not require back-propagating any gradients through the network, while the required calculations can be efficiently performed using an embedded CPU, rendering the whole process extremely efficient.

However, WI suffers from significant limitations, that hinders its application in many real-world cases. First of all, WI implicitly assumes that the distribution of the features extracted from the DL model for novel categories will be unimodal. While this assumption usually holds for the distribution of classes for which the DL model was trained, there is no guarantee that this will hold for novel categories, which were never presented to the network during the training process. Furthermore, the impact of the training process on the actual performance on the network during few-shot learning has not been adequately examined in existing literature. More specifically, as we also experimentally demonstrate in this paper, there seems to be a direct connection between maintaining the variance of the embeddings around the prototypes and the generalization abilities of a representation/model on unknown classes. This is not a surprising result, since it is well known that overfitted representations almost always lead to worse generalization (after a certain point) [16], [17], [18]. This naturally leads us to the following question: Is it possible to design a representation in which the variance around the prototypes will be deliberately controlled to achieve the perfect balance between overfitting and underfitting instead of relying on early-stopping, implicit regularization or other heuristics to maintain enough variance? Also note that maintaining the variance will allow more information about the in-class similarities/dissimilarities to be encoded in the resulting
The main contribution of this paper is a novel weight imprinting method, which is capable of overcoming the aforementioned limitations. To this end, the proposed method learns a regularized embedding by maintaining the variance around the prototypes in a structured way. The proposed approach provides an effective way to directly handle novel categories with multimodal distributions, as well as natively supports few-shot learning. To the best of our knowledge, in this paper we propose the first variance-preserving approach for performing imprinting-aware few-shot learning.

The rest of this paper is structured as follows. First, the proposed method is derived and discussed in Section II. Then, the proposed method is evaluated and compared to regular WI under different scenarios in Section III. Finally, conclusions are drawn and future research directions are discussed in Section IV.

II. PROPOSED METHOD

The proposed method aims to learn a carefully designed feature space to more effectively support weight imprinting. To this end, a centroid-based loss, which uniformly distributes the embedding vectors within a radius $r$ around each prototype (centroid), is employed. Furthermore, to ensure that the prototypes are discriminative enough it is required that the minimum distance between two prototypes is at least $\rho > 2r$. This process is illustrated in Fig. 1. After learning a representation that fulfills the aforementioned requirements we can directly classify a new sample, perform gradient descent-free few-shot learning, detect and handle multimodal novel classes and detect intrusion to the existing classes that can lower the performance of the model.

A. Embedding Extractor Training

First, we will describe the proposed imprinting-aware training process. Let $\phi(x) \in \mathbb{R}^m$ be the output of a neural network, where $m$ is the dimensionality of the embeddings extracted from the network, when presented with an input sample $x$. Also, let $w_i$ be the prototype vector for the $i$-th class used during the training process and $X_i$ be the set of samples that belong to the class $i$. Then, to ensure that the embeddings will be uniformly distributed around each class prototype $w_i \in \mathbb{R}^m$ we define the appropriate class-induced loss as:

$$L_c = \frac{1}{N} \sum_{i=1}^{N_C} \sum_{x \in X_i} (||\phi(x) - w_i||_2 - \alpha r)^2,$$

where $N$ is the total number of training samples, $N_C$ is the total number of training classes, $||\cdot||_2$ denotes the $l^2$ norm of a vector and $\alpha \in [0, 1]$ is a number drawn uniformly from the range $[0...1]$. During the optimization a different random value is drawn for $\alpha$ for each sample and iteration, leading to a uniform distribution of the embeddings within a radius $r$ from each $w_i$. Even though this process does not ensure that the full space around $w_i$ will be occupied, it ensures that the embeddings will be sampled uniformly at various radiuses around the corresponding center, significantly improving the generalization abilities of the representation, as we will demonstrate later in Section III. Note that by setting $r = 0$, the loss $L_{\text{class}}$ degenerates to the regular center loss [19]. Furthermore, to further model the uncertainty regarding the class prototypes, we can use Gaussian noise to corrupt the prototypes as:

$$\tilde{w}_i = w_i + \mathcal{N}(0, \sigma).$$

At the same time, each prototype $w_i$ is required to be at a distance of at least $\rho$ from each other prototype (to ensure that there is no overlapping between the hyperspheres that enclose the embeddings of each class). To this end, we also define the prototype loss as:

$$L_p = \frac{1}{N_C(N_C - 1)} \sum_{i=1}^{N_C} \sum_{j=1, j \neq i} \max(0, \rho - ||w_i - w_j||_2).$$

Therefore, the model parameters, along with the prototypes, are optimized during the training to minimize the following loss:

$$L = L_c + \gamma L_p,$$

where $\gamma$ is a hyper-parameter parameter that alters the weight of the prototype loss (set to 1 for all the experiments conducted in this paper).

B. Classification and Few-shot Learning

To classify an input sample we can directly choose the class that corresponds to the prototype with the smaller distance to the extracted embedding $\phi(x)$. The network can be used in a similar fashion as a one trained using the softmax activation simply by using a final classification layer that calculates the membership value for each prototype/class probabilities as:

$$p_i(x) = \frac{1}{1 + ||\phi(x) - w_i||_2}.$$

It is worth noting that the probability distribution can be smoothed or sharpened by appropriately transforming it, e.g., using the softmax function with appropriately tuned temperature, if needed.

To perform few-shot learning we can simply augment the final classification layer with an additional prototype vector $w_n$ calculated as:

$$w_n = \frac{1}{|X_n|} \sum_{x \in X_n} \phi(x),$$

where $X_n$ is the set that contains the training samples for the novel category. Note that similarly to regular WI, no gradient descent-based optimization is required for extending the classifier to support novel classes. However, as we further demonstrate in Section III, the regularized nature of the learned feature space leads to significantly better performance compared to regular WI.
C. Detecting and handling multimodal novel categories

There are several ways to detect if the distribution of a novel class is indeed multimodal. In this paper, we propose using a quite simple, yet effective way: we propose directly detecting multimodal categories by clustering the embedding vectors extracted for a novel category. If we detect centers that are at distance greater than \( r \) (or any other user-defined threshold) from each other, then a hypersphere with radius of \( r \) cannot enclose the embeddings of the novel class. To address this, we can simply add one or more prototypes (according to the number of centers that are at distance greater than \( r \)) to model the distribution of the novel class. In this way, one class can be represented using more than one prototype. On the other hand, if the centers of the clusters are within a radius of \( r \), then we assume that proposed classification scheme can directly handle the distribution of the novel class (even though there is no guarantee that the distribution is not multimodal).

III. EXPERIMENTAL EVALUATION

The proposed method was evaluated using two different image datasets, the MNIST dataset [20] and the Animals with Attributes (AwA2) dataset [21], in order to measure its performance under two different settings. For the MNIST dataset the first 5 classes were used to train the model, while the remaining 5 classes were used for few-shot learning and evaluation. For the AwA2 dataset [21] the first 40 classes were used for training the model, and the rest of the classes were employed for evaluating the performance of the proposed method. The performance evaluation was repeated 5 times using different training samples for the novel classes (except for the hyper-parameter evaluation experiments) and the mean and standard deviation is reported. For the MNIST dataset the employed neural network was composed of a \( 3 \times 3 \) convolutional layer with 32 filters, followed by a \( 2 \times 2 \) max pooling layer, another \( 3 \times 3 \) convolutional layer with 64 filters, an additional \( 2 \times 2 \) max pooling layer and a fully connected layer with 256 neurons. For the AwA2 dataset we used a pretrained ResNet101 to extract feature vectors (as described in [21]) that were then fed to two fully connected layers with 2048 and 512 neurons respectively. The \( \text{relu} \) activation function was used for all the layers [22]. The models were trained using the Adam optimizer with a learning rate of \( 10^{-3} \) for 20 training epochs for the MNIST dataset and of \( 10^{-4} \) for 20 training epochs for the AwA2 dataset [23].

First, we evaluated the effect of altering the radius \( r \) on the learned representation. In Section II it was conjectured that spreading the training embeddings in a hypersphere of radius \( r \) will have a positive regularization effect on the learned representation by allowing the model to capture and better model the in-class variations. Indeed, as demonstrated in Table II, the classification accuracy increases by more than 14% for the novel split, and by 1.8% for the combined split. This confirms our hypothesis that collapsing the embeddings to the class centers, without any form of regularization, can significantly reduce the classification accuracy, especially when dealing with classes that were not seen during the training process and using powerful models that can overfit the training data.

Next, we evaluated the proposed method using a 1-shot, 2-
TABLE I

<table>
<thead>
<tr>
<th>Min. Distance $\rho$</th>
<th>Novel</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>56.28</td>
<td>77.79</td>
</tr>
<tr>
<td>2</td>
<td>56.24</td>
<td>77.42</td>
</tr>
<tr>
<td>5</td>
<td>58.53</td>
<td>78.66</td>
</tr>
<tr>
<td>10</td>
<td>61.02</td>
<td>80.06</td>
</tr>
<tr>
<td>20</td>
<td>53.82</td>
<td>76.51</td>
</tr>
</tbody>
</table>

TABLE II

<table>
<thead>
<tr>
<th>Radius $r$</th>
<th>Novel</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>61.02</td>
<td>80.06</td>
</tr>
<tr>
<td>4</td>
<td>64.51</td>
<td>80.59</td>
</tr>
<tr>
<td>5</td>
<td>69.57</td>
<td>81.55</td>
</tr>
<tr>
<td>6</td>
<td>66.86</td>
<td>78.26</td>
</tr>
</tbody>
</table>

The proposed method was also compared to the plain Weight Imprinting (WI) approach [15], using an initial scaling value of $c = 10$. Again, it was confirmed that using the proposed variance preserving approach improves the performance over simply using a center-based loss, allowing for outperforming the regular WI method on all the evaluation splits and few-shot learning setups. It is worth noting that the accuracy for all the evaluated methods is relatively low compared to the state-of-the-art, since neither WI nor the proposed method perform any kind of optimization according to a discriminative objective.

To demonstrate the ability of the proposed method to handle multimodal classes we also evaluated the proposed approach using an additional multimodal split of the MNIST dataset. This split was compiled by merging two succeeding classes into one, e.g., “0” and “1” were merged into a new class, “2” and “3” into another, and so on. Then, the three first classes (digits 0 to 5) were used for training and the remaining two of them (6 to 9) for evaluating the few-shot learning performance. The evaluation results are reported in Table IV. The employed threshold was used to detecting whether a class distribution is multimodal (by clustering the training data into two clusters and measuring the distance between the resulting centroids). If the distance of the resulting centers was greater than the specified threshold, then two prototypes were used per novel class. Again, note that the variance-preserving variant of the proposed method greatly outperforms the baseline variant (“Proposed-”), as well as using the proposed multimodal handling approach (with a correctly tuned threshold) allows for significantly improving the performance of the proposed method, outperforming all the other evaluated approaches.

Finally, we also evaluated the performance of the proposed method using a more challenging dataset, the AwA2 dataset. The results are reported in Table V. We report evaluation results only for the novel categories, since due to the small number of training samples, all the data from the training categories were used for training the model. As before, the proposed method leads to significant performance improvements over the plain WI method, while it still outperforms the HWI-methods. The smaller differences between HWI- and HWI can be possibly attributed to the the smaller learning capacity of the employed network (the risk of overfitting the representation is higher when more powerful networks are employed). Note that slightly different hyper-parameters were used for the HWI method in this experiment: $r = 20$, $t = 10$, and $\sigma = 0$.

IV. CONCLUSIONS

In this paper we proposed a novel hypersphere-based weight imprinting approach that maintains all the advantages of regular

TABLE III

<table>
<thead>
<tr>
<th>Method</th>
<th>Split</th>
<th>1-shot</th>
<th>2-shot</th>
<th>5-shot</th>
</tr>
</thead>
<tbody>
<tr>
<td>WI</td>
<td>Novel</td>
<td>52.44 ± 7.4</td>
<td>66.95 ± 4.3</td>
<td>72.51 ± 2.6</td>
</tr>
<tr>
<td>Proposed</td>
<td>Novel</td>
<td>47.46 ± 9.9</td>
<td>59.98 ± 2.6</td>
<td>66.60 ± 3.7</td>
</tr>
<tr>
<td>Proposed</td>
<td>Novel</td>
<td>57.93 ± 4.2</td>
<td>68.72 ± 5.1</td>
<td>75.20 ± 3.5</td>
</tr>
<tr>
<td>WI</td>
<td>All</td>
<td>57.51 ± 5.8</td>
<td>58.35 ± 6.4</td>
<td>64.49 ± 3.2</td>
</tr>
<tr>
<td>Proposed</td>
<td>All</td>
<td>73.27 ± 4.7</td>
<td>79.46 ± 1.5</td>
<td>82.88 ± 1.8</td>
</tr>
<tr>
<td>Proposed</td>
<td>All</td>
<td>73.66 ± 3.9</td>
<td>79.09 ± 6.0</td>
<td>84.23 ± 1.3</td>
</tr>
</tbody>
</table>

TABLE IV
MNIST MULTIMODAL: EVALUATING THE ACCURACY OF IMPRINTING METHODS ON THE NOVEL CATEGORIES.

<table>
<thead>
<tr>
<th>Method</th>
<th>Thres.</th>
<th>2-shot</th>
<th>4-shot</th>
<th>10-shot</th>
</tr>
</thead>
<tbody>
<tr>
<td>WI</td>
<td>-</td>
<td>55.81 ± 11.7</td>
<td>65.17 ± 12.3</td>
<td>78.89 ± 2.6</td>
</tr>
<tr>
<td>Proposed</td>
<td>-</td>
<td>42.07 ± 6.5</td>
<td>47.40 ± 9.6</td>
<td>55.47 ± 2.4</td>
</tr>
<tr>
<td>Proposed</td>
<td>-</td>
<td>60.95 ± 4.0</td>
<td>71.03 ± 5.5</td>
<td>75.69 ± 1.0</td>
</tr>
<tr>
<td>Proposed</td>
<td>5</td>
<td>62.36 ± 3.4</td>
<td>70.00 ± 5.3</td>
<td>75.69 ± 1.0</td>
</tr>
<tr>
<td>Proposed</td>
<td>4</td>
<td>66.47 ± 5.0</td>
<td>71.52 ± 2.3</td>
<td>75.11 ± 2.8</td>
</tr>
<tr>
<td>Proposed</td>
<td>3</td>
<td>66.78 ± 4.9</td>
<td>73.99 ± 5.6</td>
<td>82.69 ± 1.5</td>
</tr>
</tbody>
</table>

TABLE V
AWA2: EVALUATING THE ACCURACY OF IMPRINTING METHODS ON THE COMBINED NOVEL AND TRAINING CATEGORIES SPLIT.

<table>
<thead>
<tr>
<th>Method</th>
<th>1-shot</th>
<th>2-shot</th>
<th>5-shot</th>
</tr>
</thead>
<tbody>
<tr>
<td>WI</td>
<td>51.03 ± 3.71</td>
<td>61.33 ± 2.73</td>
<td>75.23 ± 1.85</td>
</tr>
<tr>
<td>Proposed</td>
<td>54.55 ± 3.31</td>
<td>68.44 ± 3.17</td>
<td>76.95 ± 2.12</td>
</tr>
<tr>
<td>Proposed</td>
<td>56.14 ± 2.70</td>
<td>70.16 ± 2.63</td>
<td>77.85 ± 1.84</td>
</tr>
</tbody>
</table>
lar WI [15], i.e., it is able to readily extend a pretrained neural network to classify samples from novel categories simply by adding new weight vectors in the final classification layer without requiring to perform any form of back-propagation to this end. At the same time, the proposed method was capable to overcome significant limitations of WI by being able to learn regularized representations that provide better generalization for classes which were not seen during the training and provide a straightforward way to directly handle novel categories with multimodal distributions. The proposed method was extensively evaluated on two image datasets, outperforming the regular WI approach. However, it is worth noting that the imprinting process is still quite behind traditional gradient descent-based learning approaches.

There are several interesting future research directions. First, even though the proposed clustering-based multi-modality detection led to adequate results, several most sophisticated methods can be used for detecting whether the distribution of a novel class is indeed multimodal. Also, to better spread the in-class samples in the volume of the hypersphere we employed a stochastic process that randomly distributes the samples in various radiiuses. However, this process ignores the actual geometry of the data. More advanced methods that take into account the actual manifold of the data, e.g., by using data from a previous layer and then distilling the extracted information into the used model [24], [25], [26], can be employed. Finally, the proposed hypersphere-based loss showed a great potential for improving regular training tasks as well. Therefore, it can be potentially successfully used even for regular classification tasks, further improving the accuracy of the corresponding models.

ACKNOWLEDGMENTS

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 871449 (OpenDR). This publication reflects the authors’ views only. The European Commission is not responsible for any use that may be made of the information it contains.

REFERENCES