Paired Training Framework for Time-Constrained Learning

Jung-Eun Kim
Computer Science
Yale University
New Haven, CT, USA
jung-eun.kim@yale.edu

Richard Bradford
Commercial Avionics Engineering
Collins Aerospace
Cedar Rapids, IA, USA
richard.bradford@collins.com

Max Del Giudice
Computer Science
Yale University
New Haven, CT, USA
max.delgiudice@yale.edu

Zhong Shao
Computer Science
Yale University
New Haven, CT, USA
zhong.shao@yale.edu

Abstract—This paper presents a design framework for machine learning applications that operate in systems such as cyber-physical systems where time is a scarce resource. We manage the tradeoff between processing time and solution quality by performing as much preprocessing of data as time will allow. This approach leads us to a design framework in which there are two separate learning networks: one for preprocessing and one for the core application functionality. We show how these networks can be trained together and how they can operate in an anytime fashion to optimize performance.

I. INTRODUCTION

A Cyber-Physical System (CPS) interacts with the physical world and often faces resource – especially timing – constraints depending on the state of its dynamic environment. Moreover, in a CPS, software components’ interactions are carefully controlled, therefore determinism and predictability are important requirements. Meanwhile, CPSES are expected to evolve by obtaining intelligence from emerging learning frameworks to achieve advanced autonomy [6]. In contrast with current CPS where determinism is of the utmost importance, learning technologies are intrinsically non-deterministic. This issue can hinder a CPS equipped with learning modules from managing its constituent learning components in a controllable manner.

This paper presents a framework for designing learning applications to operate in time-constrained systems. We consider applications in which the input data may be imperfect but may be amenable to refinement by preprocessing. We also consider environments in which the call for an inference may arise with little advance warning, with a response then needed no later than a given deadline. Given these assumptions, we consider a learning-enabled system that operates in an anytime fashion, where a usable answer is derived quickly but is improved by additional processing as time allows.

We assume that the core application runs to completion with relatively predictable performance. In contrast, at least over the ranges of interest, additional time spent preprocessing the input data will result in monotonic improvement of the quality of the system’s output. As a result, we consider it useful to think of the system as being composed of two separate networks – a preprocessor and a target network. The preprocessor processes input data and feeds its output (processed data) to the target network which provides the functionality of interest. Additional processing may be performed as time allows.

Our framework of the system as including separate preprocessing and target networks raises interesting questions as to how best to train such a system. In particular, if we are concerned with the performance of the overall system, how should we train each of the two networks? Note that our goal lies in exploring the practicality of the paired training framework, not in achieving state-of-the-art performance of any individual or entire network.

This work is supported in part by NSF grants 1945541, 1763399, and 1521523. All views expressed here are those of the authors and not necessarily those of sponsors.

To illustrate the various design issues associated with our general framework, we consider two possible example applications for the autonomous vehicle domain. One application includes a classification neural network that classifies traffic sign images; the other predicts the best angle of the steering wheel based on images of the upcoming segment of road. Each application has a denoising (i.e., noise-removing) network, so the target network can keep receiving (possibly) improved data from the denoising network as time allows. Removal of noise from the input data would increase the likelihood that the target network generates a high-quality output. When the inputs are observed in poor weather conditions, e.g., fog, rain or snow, the benefit from a preprocessor (denoiser, in this case) should be especially significant.

We illustrate the implementation of our example two-network applications by describing each one’s training and operational phases. We show how the preprocessing and target networks can be trained so as to optimize the performance of the overall system. We show that our proposed Paired Training approach results in better system performance than an alternative approach of training the two networks separately. For the operational phase, we illustrate the efficient use of processing time, so that the system achieves anytime performance, i.e. it provides a usable answer initially, with improved results when time allows for additional processing [12], [17], [23]. To the best of our knowledge, this is the first framework that provides anytime performance by employing two different networks working in tandem.

II. SYSTEM MODEL

A. Overview

We propose a framework consisting of two learning networks – one network refines the input that is passed to the other network, which is ultimately responsible for executing the given target task. The network executing the target functionality is called the target network. A target network can provide one-time prediction from raw input. However, by employing an additional network called the preprocessor, the target network can take advantage of potentially improved inputs from the preprocessor as shown in Fig. [1].

During training, the two networks interact so each network can learn the counterpart’s behavior. The interactions are detailed in various training schemes that we propose in this paper, and the experimental results show that these interactions improve the overall system performance, when compared to the case of no interaction. Fig. [2] shows an abstract view of our proposed framework with a denoising and classifying network example.

B. System Description

1. Target Network, T: Take an input from the problem domain and execute the target functionality. Target functionality can be classification, regression, clustering, etc. T : X → Y, where X is a (general) problem domain, and Y is the output space, e.g., classes, values between [0, 1], etc. Because X and Y are generally

...
As parts of a larger system (e.g., classifying noisy images), we associate their training processes to optimize system performance, by encoding this insight through their respective loss functions.

The preprocessor can either try to solely optimize its goal (train independently), or it can receive feedback from the target network, by running the target on the preprocessed outputs and checking the target loss (the preprocessor loss is now dependent on the target loss). Likewise, the classifier can be trained on non-processed clean data, or it can be trained on the preprocessor’s output data. We detail such dependent/independent loss functions below. Henceforth, $x$ indicates noisy inputs, $\hat{x}$ indicates clean (non-noisy) labels as a reference, and $c$ indicates the (task)-label for $x$.

- **Training preprocessor**: When training preprocessor independently or dependently (to target network’s loss) the following protocols are used, respectively:
  - Independent training: Train the preprocessor with the standard mean squared error (MSE) loss which counts the difference between the objective (reference) and a predicted value:
    \[
    L = L_{\text{MSE}}(P(x), \hat{x}) = (P(x) - \hat{x})^2
    \]
  - Dependent training: Feed the prediction $\hat{x}$ into a target network and use the resulting performance loss $L_{\mu}$ (dependent upon the target task) to inform the preprocessor training. We call this protocol as Pair Target Feedback (PTF). Assuming $x$ has appropriate task-label $c$, we define $L$ as:
    \[
    L = L_{\text{MSE}}(P(x), \hat{x}) + \lambda_{\mu}L_{\mu}(T \circ P)(x), c)
    \]
    where $\lambda_{\mu}$ is the weight of the classifier loss relative to the MSE loss. The precise formulation of $L_{\mu}$ is contingent upon the goal of the target network.

- **Training target network**: We consider two protocols:
  - Independent training: Train the target network with clean input in isolation from the preprocessor:
    \[
    L = L_\mu(T(\hat{x}), c)
    \]
  - Dependent training: Use a preprocessor to process the noisy input, and then run the target network on the processed output:
    \[
    L = L_\mu((T \circ P)(x), c)
    \]

**B. Interleaved Training Framework**

Given the proposed system where the target performance is dependent on the preprocessor output, we discovered that training the preprocessor and target network by turns, which we call Interleaved Training (see Fig. 2), and pairing one another’s loss results in improved system performance. It stems from the fact that even though in the course of one’s training the counterpart’s behavior (performance loss) is taken into account, if the counterpart is already pre-trained (independently too mature) or is not trained at all (too immature), the performance is not promising. As a result, we have found that the following training cases do not show competitive performance: (a) Preprocessor and target network are separately trained; (b) Target network has been separately trained although it is involved in preprocessor’s training procedure. With this motivation in mind, we devised the following interleaved training techniques. The following training schemes connect the training processes of the preprocessor and target network in different ways. Let $2E$ be the number of epochs for an entire training procedure.

- **Alternating**: (i) Train target network independently for $E$ epochs,
  (ii) Train preprocessor for $2E$ epochs dependently with “frozen” (i.e., keeping the weights) target network and PTF loss (see [2]),
and then (iii) Train target network for $E$ epochs dependently with preprocessor output. See Fig. 2(a).

- MERGE1: (i) Train target network independently for $E$ epochs, (ii) Train preprocessor for $E$ epochs dependently with frozen target network and PTF loss, and then (iii) Train both networks, using the preprocessor output to train the target network and PTF loss to train the preprocessor. See Fig. 2(b).

- MERGE2: (i) Train preprocessor for $E$ epochs, (ii) Train target network for $E$ epochs with frozen preprocessor, and then (iii) Train both networks, using the preprocessor output to train the target network and PTF loss to train the preprocessor. See Fig. 2(c).

By training the target network directly with the preprocessor output, and using feedback from the target network, we optimize the whole system rather than each network individually.

Our aim does not lie in developing an optimal paired training scheme, rather we intend to show the impact of paired training approaches by comparing them with non-paired approaches. To achieve the goal, through the experiments, we answer the following questions: Is the entire system performance aligned with the individual performance of the component networks, preprocessor and target network? How do we train and optimize the component networks to perform well in tandem? How do we optimize anytime performance?

IV. EXPERIMENTS

A. Evaluation Setup

1) Applications: While the training scheme with preprocessor and target network generalizes to multiple applications, our experiments examine the case where the preprocessor is a denoising network and the target network is either a classification or regression network:

- **Preprocessor (Denoising):** removes different types of noise from an image. The denoising network shares some architectural similarities with one in [8]. Our denoiser begins with a learning rate of $10^{-4}$, reduced to $10^{-5}$ after 100 (= $E$) epochs, as the entire training lasts 200 epochs. Depending on the training scheme, the loss function is either represented by (1) or (2). In (2), we empirically determine 0.25 to be a good value for $\lambda_p$. The denoiser is trained for 6 iterations since improvements level off after this point.

- **Target network (Classification):** contains 43 traffic sign classes. The classification target network is based on an 18-layer ResNet [9]. Our ResNet implementation begins with a learning rate of $10^{-4}$, reduced to $10^{-5}$ after 100 epochs of training. In the loss function, $L_p$ is cross entropy with logits. The standard cross entropy loss is augmented with a L2-regularization term with weight $\lambda = 10^{-4}$.
4) Performance Measures:

- System performance: For the GTSRB and CIFAR-10 datasets, we use Top-1 classification accuracy. For the SteeringPattern dataset, we observe the mean-square error. We evaluate the performance with respect to each iteration of the preprocessor.
- Preprocessor performance: We independently evaluate the preprocessor’s performance by computing the average mean squared error over noisy test images. We evaluate the performance with respect to each iteration of the preprocessor.
- Target network performance: For the classification network, we evaluate performance by computing average Top-1 accuracy over clean (non-noisy) test images. For the regression network, we compute average mean squared error over clean test images.

5) Approaches: In addition to the paired training approaches proposed in Section III-B, Alternating, Merge1, and Merge2, we evaluate the following baseline approaches for comparison:

- NoPreprocessor: target network runs without preprocessor support. Since Anytime performance is realized by the support from a preprocessor, any further performance improvement is not expected - only a single result is expected.
- Separate: target network and preprocessor are independently trained with no knowledge about each other. Preprocessor conforms to loss function (1) and target network does to (3). For the classification network, \(L_p\) is cross entropy with logits; for the regression network, \(L_p\) is mean squared error.
- TrainedTarget: preprocessor is trained with a pre-trained target network (which has been independently trained) according to loss function as shown in (5). Target network’s weights stay the same.

B. System Performance

To begin, in Fig. 5 the impact of the preprocessor is seen by comparing NoPreprocessor with the later iteration outputs of the other approaches. By having a preprocessor we can expect further improved accuracy. With no support from any preprocessor, the result of NoPreprocessor is the only output that we can expect.

We notice the impact of employing paired training schemes, which is shown by comparing Separate and Alternating, Merge1, and Merge2. As explained in Sec. IV-A, in Alternating, Merge1, and Merge2, either the preprocessor or target network considers the other in its training procedure, while in Separate, the two networks are trained independently. The distinction between Separate and the other schemes shows the positive contribution of paired training to overall system performance. That is, generally and independently...
pre-trained networks are not expected to provide optimal performance if they are supposed to interact with each other in inference time.

1) Impact of Target Task: In order to determine the generalizability of this framework over various potential target networks, we trained a regression network in addition to the classification network. Our RegressionNet takes as input an image from the front-facing camera of a vehicle, and then performs steering angle prediction. The model is trained on the STEERINGPATTERN dataset. Results are shown in Fig. 5(c) and 5(d). Note that the first iteration (no iterations of the denoiser) is omitted, as it is an order of magnitude higher than the following iterations, and it compresses the results shown in the figures.

We notice ALTERNATING and MERGE1 perform worse than SEPARATE in earlier iterations, but excel by the final iteration. Likewise, MERGE2 displays more steady performance, outperforming SEPARATE for each iteration, and roughly matching SEPARATE by the final iteration. This is particularly notable in the Gaussian noise case. While this trend is much more visible in the regression context, it is present in the classification context as well—this is, we see MERGE2 outperform MERGE1 and ALTERNATING for the first iteration or two, after which MERGE1 and ALTERNATING tend to surpass MERGE2.

For ALTERNATING and MERGE1, the results are showing that training the target network first, and using the trained target network to provide feedback across the rest of the training process, directs the gradient descent process towards the ultimate goal of classification/regression rather than the ancillary (denoiser) goal of reducing mean squared error. This leads to ultimately superior performance by the final iteration. However, leading with training the denoiser, as in MERGE2, translates to a more stable and quickly converging training process, at the cost of final performance.

The result indicates that there are tradeoffs implicit in the proposed interleaved approaches with respect to anytime performance. Namely, better performing earlier iterations corresponds with a less optimal final iteration, whereas better performing later iterations corresponds with a worse-performing earlier iterations. This can be more broadly related with the convergence of an “anytime system” such as the one proposed in the paper. Our experimental setup remained largely unchanged between classification and regression - with a longer, more careful training procedure, ALTERNATING and MERGE1 could excel over MERGE2 in most iterations, similar to the classification case.

2) Impact of Noise Complexity: Comparing the accuracy curves in Fig. 5, the noise type impacts the potential benefits of paired training. The more complex the noise type, the more significant the improvement in performance. GAUSSIAN noise is relatively complex, given its randomized nature and application to each pixel, whereas SYNTHETIC noise is simpler. In GAUSSIAN noise curves, all paired training schemes exceed SEPARATE, both in final performance and in earlier iterations. For SYNTHETIC noise, the paired training schemes also outperform SEPARATE, but the improvement is slightly less significant. The complexity of denoising is responsible for this variance. For more complex noise, the denoiser is more likely introducing artifacts or impacting the performance of the classifier. Then, training the classifier with output from the denoiser or the denoiser with classifier feedback allows the system to optimize with knowledge of the artifacts, resulting in a substantial performance boost.

3) Dataset Impact: We examined the performance of paired training schemes across the CIFAR-10 and GTSRB datasets on Gaussian noise (see Fig. 6). We found similar trends across both datasets: ALTERNATING and MERGE1 ultimately outperform MERGE2, but MERGE2 displays stronger performance in the earlier iterations.

We do note that the gap between the best approach and SEPARATE for the final iteration of CIFAR-10 and GTSRB are of different orders of magnitude. Indeed, there is a accuracy gap of 0.01 between ALTERNATING and SEPARATE on the GTSRB dataset, while there is a 0.08 accuracy gap between ALTERNATING and SEPARATE. We attribute this difference to complexity of the target task – the CIFAR-10 images are more complex than those in GTSRB, and they have lower resolution. The different active ranges on the Y-axes of each case reflect the fact. Consequently, the application of Gaussian noise impacts the performance of the classifier more severely, making the performance of the classifier much more tied to the performance of the denoiser. In this situation, a form of interleaving is highly beneficial.

C. Independent Performance

The proposed framework trains the two networks to boost the system performance through paired training approaches and loss protocols. In the proposed system, each individual network does not necessarily display optimal performance respectively, since the paired loss protocol and training approaches optimize for system performance rather than individual network performance. We show the cost paid for overall performance by looking at the individual performance of the two component networks: classification performance of the target network on clean inputs, and mean squared error of the denoiser.

![Fig. 6: Comparison of training approaches on different data sets with GAUSSIAN noise.](image)
1) Target Performance: The impact of paired training on each classifier’s independent performance, i.e., performance on clean inputs. Table 1 shows how the paired training and separate training approaches train the target networks over Gaussian and Synthetic noise. We can see that the individual target networks produced by the four paired training approaches perform worse than the SEPARATE and TRAINEDTARGET target networks. This result corresponds to the training processes for each paired approach. TRAINEDTARGET trains the target network independently, so the performance should be roughly equivalent to SEPARATE. Conversely, ALTERNATING, MERGE1, and MERGE2 all use preprocessor output to train the target at some point. Thus, the target networks for these approaches become optimized with respect to the corresponding denoising network, resulting in a small negative impact on their performance over clean data.

2) Preprocessor Performance: The independent performance of the denoiser is also affected by the paired training scheme. Contrasting with the independent performance of the target network, paired training approaches improve the independent performance of the denoiser. The feedback provided by the target helps the denoiser learn high-level information about the images being denoised. Looking at the specific approaches, those which begin by training the target and use that target to train the denoiser (ALTERNATING, MERGE1, and SEPARATE) have the most improved performance. MERGE2 only training the denoiser with paired loss at the end of training has the weakest performance.

V. RELATED WORK

For problems involving temporal sequences of data, a model must be able to encode dependencies across multiple timesteps. RNNs can model these sequential-type data: e.g., text-prediction, speech recognition, or handwriting recognition. What differentiates RNNs from typical feed-forward neural networks is the existence of internal states that encode sequences of inputs that have occurred earlier. This is a form of memory that enables RNNs to process sequential data. Critical to the understanding of RNNs is that the learnable parameters, input, state, and output at a given timestep, are shared between iterations. Were parameters not shared between iterations, the number of parameters in the model would explode for any sequence of appreciable length, making training intractable.

Many recent architectures have combined RNN and convolutional neural network (CNN) structures: basic LSTM components with convolutions [11], [14], [16]: more complex LSTMs [15]: dilated convolutions [4], and quasi-recurrence [3]. The authors in [16] designed recurrent convolutional layers for classification. The work in [11] developed a deep-recurrent convolutional network for image super-resolution. A single RCL to learn complex feature maps is used not to introduce large numbers of parameters.

Image restoration has long been a central problem in low-level image processing. Procedures such as K-SVD [1], BM3D [5], the LRA-SVD method [7], and the LPG-PCA method [20] exploit the structured nature of image data, deriving information from groups of image patches to fill-in missing or obscured data. More recently, neural network based approaches have begun to surpass the more traditional approaches discussed above. Initially, autoencoders [22] and convolutional neural networks [10] showed promising results. More recently, deeper convolutional networks such as ResNets [21], GANs [15] and RNNs [8] have all broken numerous existing benchmarks for denoising and super-resolution.

VI. CONCLUSION

We proposed a framework employing two networks, a preprocessor and a target network, working in tandem; a raw input goes into a preprocessor, and the target network generates the final output. Several paired and interleaved training approaches, along with a joint loss mechanism, are compared to a baseline of independently trained networks. Pairing the training processes using these mechanisms results in better system performance than training each network in isolation. Further explorations into confidence levels at each iteration to obtain a strict Anytime curve, hyperparameters on paired loss functions, and different variations of interleaving mechanisms for paired training approaches will be interesting future directions.

REFERENCES