Lawrence Berkeley National Laboratory
Recent Work

Title
Learning to classify from impure samples with high-dimensional data

Permalink
https://escholarship.org/uc/item/50v1k1s5

Journal
Physical Review D, 98(1)

ISSN
2470-0010

Authors
Komiske, PT
Metodiev, EM
Nachman, B
et al.

Publication Date
2018-07-16

DOI
10.1103/physrevd.98.011502

Peer reviewed
Learning to classify from impure samples with high-dimensional data

Patrick T. Komiske,1,* Eric M. Metodiev,1,‡ Benjamin Nachman,2,† and Matthew D. Schwartz3,§
1Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
2Physics Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA
3Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA

(Received 7 February 2018; revised manuscript received 14 April 2018; published 16 July 2018)

A persistent challenge in practical classification tasks is that labeled training sets are not always available. In particle physics, this challenge is surmounted by the use of simulations. These simulations accurately reproduce most features of data, but cannot be trusted to capture all of the complex correlations exploitable by modern machine learning methods. Recent work in weakly supervised learning has shown that simple, low-dimensional classifiers can be trained using only the impure mixtures present in data. Here, we demonstrate that complex, high-dimensional classifiers can also be trained on impure mixtures using weak supervision techniques, with performance comparable to what could be achieved with pure samples. Using weak supervision will therefore allow us to avoid relying exclusively on simulations for high-dimensional classification. This work opens the door to a new regime whereby complex models are trained directly on data, providing direct access to probe the underlying physics.

DOI: 10.1103/PhysRevD.98.011502

Data analysis methods at the Large Hadron Collider (LHC) rely heavily on simulations. These simulations are generally excellent and allow us to explore the mapping between truth information (particles from collisions) and observables (reconstructed momenta and energies). In particular, simulations let us train complex algorithms to extract the truth information from the observables. Machine learning methods trained on low-level inputs have been developed for collider physics [1] to identify boosted $W/Z$/Higgs bosons [2–8], top quarks [9–13], $b$-quarks [14–16], and light quarks [17–20], to remove noise [21], and to emulate particle interactions with calorimeters [22–24]. These new methods achieve excellent performance by exploiting subtle features of the simulations, which are presumed to be similar to the features in the data. Unfortunately, the simulations are known to be imperfect. This is particularly true for subtle features in high dimensions, as illustrated clearly for boosted $W$ bosons in Ref. [5] and by the need for non-negligible corrections (“scale factors”) to be applied to multivariate classifiers used by the current LHC experiments (see e.g. Refs. [25–32]). Thus, it is natural to question the performance of machine learning algorithms trained on simulations as we know that if a model is trained on unphysical artifacts, this is what the model will learn. This objection certainly has merit, as the power of these methods for physics applications stems precisely from their ability to find features that we do not fully understand and cannot easily interpret.

Data-driven approaches avoid the pitfalls of relying on simulations in experimental analyses. For simple observables, such as the invariant mass of a photon pair, a traditional experimental approach has been to perform sideband fits directly to the data. This avoids relying on the simulation altogether. Unfortunately, most of the sophisticated discrimination techniques developed in recent years use full supervision, where truth information is needed in order to train the classifier. However, real data generally consist only of mixed samples without truth information, arising from underlying statistical or quantum mixtures of two classes (henceforth referred to as “signal” and “background”). Occasionally one can find a small region of phase space where the signal or background is pure, but these regions are generally sparsely populated and may not produce representative distributions. Recent work on weak supervision [33] allows classifiers to be trained using only the information available from mixed samples. Two weakly supervised paradigms tailored to physics applications are learning from label proportions (LLP) [34] and classification without labels (CWoLa) [35]. Reference [34] considered the problem of discriminating the radiation pattern of quark from gluons ($q/g$) using three standard observables and showed how to achieve fully
supervised discrimination power by using LLP with two samples of different but known quark fractions. In Ref. [35], it was shown that the proportions are not necessary for training since the likelihood ratio of the mixed samples is monotonically related to the signal/background likelihood ratio, the optimal binary classifier for signal vs background.

One potential objection to the weak-learning demonstrations in Refs. [34–36] is that the dimensionality of the inputs used is small. Indeed, for a one-dimensional discriminant one can extract the exact pure distributions from mixed samples using the fractions. It is not obvious that weak supervision will succeed when trained on high-dimensional inputs where the feature space may be sparsely populated. Indeed, the most powerful modern methods are trained on high-dimensional, low-level inputs, where numerically approximating and weighting the probability distribution is completely intractable. These deep learning techniques can expose subtle correlations in many dimensions which are also much harder to model than simple low-dimensional features.

In this paper, we demonstrate that weak supervision can approach the effectiveness of full supervision on complex models with high-dimensional inputs. As a concrete illustration, we use an image representation to distinguish the radiation pattern of high-energy quarks from gluons (“jet images” [2]). Convolutional neural networks (CNNs) are applied to the quark and gluon jet images, where the dimensionality of the inputs is \( O(1000) \) and simulation mismodeling issues are a challenge [25,37–43]. We find that CWoLa more robustly generalizes to learning with high-dimensional inputs than LLP, with the latter requiring careful engineering choices to achieve comparable performance. Though we use a particle physics problem as an example, the lessons about learning from data using mixtures of signal and background are applicable more broadly.

We begin by establishing some notation and formulating the problem. Let \( \mathbf{x} \) represent a vector of observables (features) useful for discriminating two classes we call signal (S) and background (B). For example, \( \mathbf{x} \) might be the momenta of observed particles, calorimeter energy deposits, or a complete set of observables [7,8]. In fully supervised learning, each training sample is assigned a truth label such as 1 for signal and 0 for background. Then the fully supervised model is trained to predict the correct labels for each training example by minimizing a loss function. For a sufficiently large training set, an appropriate model parameterization, and a suitable minimization procedure, the learned model should approach the optimal classifier defined by thresholding the likelihood ratio.

Data collected from a real detector do not come with signal/background labels. Instead, one typically has two or more mixtures \( M_a \) of signal and background with different signal fractions \( f_a \), such that the distribution of the features, \( p_{M_a}(\mathbf{x}) \), is given by

\[
p_{M_a}(\mathbf{x}) = f_a p_S(\mathbf{x}) + (1 - f_a) p_B(\mathbf{x}),
\]

where \( p_S \) and \( p_B \) are the signal and background distributions, respectively. Weak supervision assumes sample independence, that Eq. (1) holds with the same distributions \( p_S(\mathbf{x}) \) and \( p_B(\mathbf{x}) \) for all mixtures. Although in most situations sample independence does not hold perfectly (see e.g. Ref. [44]), it is often a very good approximation (cf. Table Ref. II below).

LLP uses any fully supervised classification method and modifies the loss function to globally match the signal fraction predicted by the model on a batch of training samples to the known truth fractions \( f_a \). Breaking the training set into batches, normally done to parallelize training, takes on a new significance with LLP since the loss function is evaluated globally on each batch. The batch size, which for LLP we define as the number of samples drawn from each mixture during one update of the model, is a critical hyperparameter of LLP.

The loss functions we use for LLP differ from those in Ref. [34]. Analogous to the mean squared error (MSE) loss function for fully supervised (or CWoLa) training, we introduce the weak MSE (WMSE) loss for the LLP framework:

\[
\ell_{WMSE} = \sum_a \left( f_a - \frac{1}{N} \sum_{i=1}^{N} h(\mathbf{x}_i) \right)^2,
\]

where \( N \) is the batch size, \( a \) indexes the mixed samples, and \( h \) is the model. Analogous to the cross entropy, we also introduce the weak cross-entropy (WCE) loss:

\[
\ell_{WCE} = \sum_a \text{CE} \left( f_a, \frac{1}{N} \sum_{i=1}^{N} h(\mathbf{x}_i) \right),
\]

where \( \text{CE}(a, b) = -a \log b - (1 - a) \log(1 - b) \). One caveat we discovered while exploring LLP is that the range of \( h(\mathbf{x}) \) must be restricted to [0, 1], otherwise the model falls into trivial minima of the loss function. We also observe the effect of model outputs becoming effectively binary at 0 and 1, necessitating additional care to avoid numerical precision issues.

CWoLa classifies two mixtures, \( M_1 \) and \( M_2 \), from each other using any fully supervised classification method. The resulting classifier is then used to directly distinguish the original signal and background processes. Amazingly, the CWoLa classifier asymptotically (as the amount of training data increases) approaches an ideal classifier trained on pure samples [35,45,46]. CWoLa does not require that the fractions \( f_a \) are known for training (the fractions on smaller test sets can be used to calibrate the classifier operating points). The CWoLa framework has the nice property that
dimensional inputs, we simulate diluting their purity. The key features of CWoLa and LLP are than two are available they can be pooled at the cost of CWoLa presently only works with two mixtures; if more smoothly approaches the fully supervised paradigm.

<table>
<thead>
<tr>
<th>Property</th>
<th>LLP</th>
<th>CWoLa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatible with any trainable model</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>No training modifications needed</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Training does not need fractions</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Smooth limit to full supervision</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Works for &gt;2 mixed samples</td>
<td>✓</td>
<td>?</td>
</tr>
</tbody>
</table>

As the samples approach complete purity \((f_1 \rightarrow 0, f_2 \rightarrow 1)\) it smoothly approaches the fully supervised paradigm. CWoLa presently only works with two mixtures; if more than two are available they can be pooled at the cost of diluting their purity. The key features of CWoLa and LLP are compared in Table I. Note that no learning is possible with either method as \(f_1 \rightarrow f_2\).

To explore weak supervision methods with high-dimensional inputs, we simulate \(Z+q/g\) events at \(\sqrt{s} = 13\) TeV using \textsc{Pythia} 8.226 [47] and create artificially mixed samples with various quark (signal) fractions. Jets with transverse momentum \(p_T^j \in [250, 275]\) GeV and rapidity \(|y| \leq 2.0\) are obtained from final-state, non-neutrino particles clustered using the anti-\(k_t\) algorithm [48] with radius \(R = 0.4\) implemented in \textsc{FastJet} 3.3.0 [49]. Single-channel, \(33 \times 33\) jet images [2,3,17] are constructed from a patch of the pseudorapidity-azimuth plane of size \(0.8 \times 0.8\) centered on the jet, treating the particle \(p_T\) values as pixel intensities. The images are normalized so the sum of the pixels is 1 and standardized by subtracting the mean and dividing by the standard deviation of each pixel as calculated from the training set.

All instantiations and trainings of neural networks were performed with the python deep learning library Keras [50] with the TensorFlow [51] backend. A CNN architecture similar to that employed in Ref. [17] was used: three 32-filter convolutional layers with filter sizes of \(8 \times 8, 4 \times 4,\) and \(4 \times 4\) followed by a 128-unit dense layer. Maxpooling of size \(2 \times 2\) was performed after each convolutional layer with a stride length of 2. The dropout rate was taken to be 0.1 for all layers. Keras VarianceScaling initialization was used to initialize the weights of the convolutional layers. Due to numerical precision issues caused by the tendency of LLP to push outputs to 0 or 1, a softmax activation function was included as part of the loss function rather than the model output layer. Validation and test sets were used consisting each of 50k 50:50 mixtures of quark and gluon jet images. Training was performed with the Adam algorithm [52] with a learning rate of 0.001 and a validation performance patience of 10 epochs. Each network was trained 10 times and the variation of the performance was used as a measure of the uncertainty. Unless otherwise specified, the following are used by default: exponential linear unit (ELU) [53] activation functions for all nonoutput layers, the CE loss function for CWoLa, and the WCE loss function for LLP.

The performance of a binary classifier can be captured by its receiver operating characteristic (ROC) curve. To condense the classifier performance into a single number, we use the area under the ROC curve (AUC). The AUC is also the probability that the classifier output is higher for signal than for background. Random classifiers have AUC = 0.5 and perfect classifiers have AUC = 1.0. We also confirmed that our conclusions are unchanged when using the background mistag rate at 50% signal efficiency as a performance metric instead.

As previously noted, the LLP paradigm works by matching the predicted fraction of signal events to the known fraction for multiple mixed samples. In Ref. [34], the averaging took place over the entire mixed sample. Averaging over the entire training set at once is effectively impossible for high-dimensional inputs such as jet images because the graphics processing units (GPUs) that are needed to train the CNNs in a reasonable amount of time typically do not have enough memory to hold the entire training set at one time. Hence, the ability to train with batches is highly desirable for using LLP with high-dimensional inputs.

There are many tradeoffs inherent with choosing the LLP batch size. Smaller batch sizes are susceptible to shot noise in the sense that the actual signal fraction on that batch may differ significantly from the fraction for the entire mixed sample, an effect which decreases as the batch size increases. Smaller batch sizes result in longer training times per epoch (because the full parallelization capabilities of the GPU cannot be used) but often require fewer epochs to train. Larger batch sizes have shorter training times per epoch but typically require more epochs to train. For CWoLa, the batch size plays the same role as in full supervision, with the

![FIG. 1. The AUC and training time of CWoLa (solid) and LLP (dashed) as the batch size is varied. Training times are measured on an NVIDIA Tesla K80 GPU using CUDA 8.0, TensorFlow 1.4.1, and Keras 2.1.2. AUC is a measure of classifier performance and is 1 for a perfect classifier and 0.5 for a completely random one.](image-url)
TABLE II. AUCs for training with CWoLa and LLP on Z + jet and dijet samples as well as on artificial mixtures of Z + g and Z + q samples. The error given is the interquartile range. There is no significant difference in classifier performance between the naturally mixed (Z + jet vs dijets) samples and the artificially mixed (Z + q/g) samples with the same signal fractions.

<table>
<thead>
<tr>
<th>Learning</th>
<th>Sample</th>
<th>AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWoLa</td>
<td>Z + jet vs dijets</td>
<td>0.8626 ± 0.0020</td>
</tr>
<tr>
<td></td>
<td>Artificial Z + q/g</td>
<td>0.8621 ± 0.0019</td>
</tr>
<tr>
<td></td>
<td>Z + jet vs dijets</td>
<td>0.8544 ± 0.0019</td>
</tr>
<tr>
<td>LLP</td>
<td>Artificial Z + q/g</td>
<td>0.8549 ± 0.0018</td>
</tr>
</tbody>
</table>

performance being largely insensitive to it but the total training time varying slightly. These tradeoffs are captured in Fig. 1, which shows both the performance and training time for CWoLa and LLP models as the batch size is swept in powers of two from 64 to 16384, trained on two mixtures with \( f_1 = 0.2 \) and \( f_2 = 0.8 \). The expected independence of CWoLa performance and the degradation of LLP performance for low batch sizes can clearly be seen. The training time curves are concave with optimum batch sizes toward the middle of the swept region. Based on this figure, we choose default batch sizes of 4000 for LLP and 400 for CWoLa.

In order to explore a slightly more realistic scenario than artificially mixing samples from the same distribution of quarks and gluons, we generate Z + jet and dijet events with the same generation parameters and cuts as described previously. These “naturally” mixed samples have quark fractions \( f_{Z+jet} = 0.88 \) and \( f_{dijets} = 0.37 \). The signal and background fractions have been systematically explored for these and many other processes in Ref. [54]. As indicated by Table Ref. II, there is no significant difference in performance on the naturally mixed or artificially mixed samples. Hence, artificially mixed samples are used in the rest of this study in order to evaluate weak supervision performance at different quark purities.

Figure 2 compares CWoLa and LLP performance for various quark/gluon purities as a function of the number of training samples. Each network is trained using two samples, one with quark fraction \( f_1 \) and the other with quark fraction \( f_2 = 1 - f_1 \). Each point in the figure is the median of 10 independent network trainings and the error bars show the 25th and 75th percentiles. Full supervision performance corresponds to CWoLa with \( f_1 = 0 \). The most important takeaway from Fig. 2 is that we have achieved good performance with both weak supervision methods over a large variety of sample purities and training sample sizes. We also see that CWoLa consistently outperforms LLP and continues to get better as additional training samples are used, likely a result of the increasingly populated feature space, whereas LLP performance tends to level off. It should be noted that given the binary output nature of LLP models, classifiers trained in this way effectively come with a working point and sweeping the threshold to produce a ROC curve may not be ideal. The purity/data tradeoff analysis of Fig. 2 can provide valuable information for practical applications of weak supervision methods in physics, particularly in cases where more data can be acquired at the expense of worsening sample purity.

The sensitivity of LLP to different choices of loss function and activation function was examined. We studied the choices of the symmetric squared loss of Eq. (2) and the weak cross-entropy loss of Eq. (3) with rectified linear unit (ReLU) [55] and ELU activation functions. We found a significant improvement in LLP classification performance in using ELU activations instead of ReLU activations, particularly at high signal efficiencies. The choice of loss function was found to be less important than the choice of activation function, but minor improvements in AUC were observed with the WCE loss function over WMSE. We also studied the dependence of CWoLa on the choice of activation function and found consistent performance between ELU and ReLU activations. These results justify our default choices of ELU activation and WCE loss functions. With the choice of ELU activation, LLP achieves almost the same performance to our CWoLa-trained network near the operating point with equal signal and background efficiencies. We suspect this is a result of the tendency of LLP to output binary predictions (near 0 or 1) rather than a continuous output that can be easily thresholded.
Lastly, LLP has the potential advantage over the present implementation of CWoLa that it can naturally encompass multiple mixed samples with different purities. While in principle adding more samples should help, it is not obvious whether the network will effectively take advantage of them. Indeed, we did not find significant improvement to LLP when adding additional samples with intermediate purities, even after significant, dedicated architecture engineering.

In conclusion, we have shown that machine learning approaches using very high-dimensional inputs can be trained directly on mixtures of signal and background, and therefore on data. This addresses one of the main objections to the use of modern machine learning in jet tagging: sensitivity to untrustworthy simulations. We have implemented and tested weakly supervised learning with both LLP and CWoLa, finding that for the quark/gluon discrimination problem considered here CWoLa outperforms LLP and is less sensitive to particular hyperparameter choices. We have developed a method for training LLP with high-dimensional inputs in batches and demonstrated that the batch size is a critical hyperparameter for both performance and training time. Given any fully supervised classifier, CWoLa works “out-of-the-box,” whereas LLP requires additional engineering to achieve good performance and is generally harder to train. Nonetheless, the success in using both of these weak supervision approaches on high-dimensional data is encouraging for the future of modern machine learning techniques in particle physics and beyond.

**ACKNOWLEDGMENTS**

The authors would like to thank Lucio Dery and Francesco Rubbo for collaboration in the initial stages of this work. We are grateful to Jesse Thaler for helpful discussions. P. T. K. and E. M. M. would like to thank the MIT Physics Department for its support. Computations for this paper were performed on the Odyssey cluster supported by the FAS Division of Science, Research Computing Group at Harvard University. This work was supported by the Office of Science of the U.S. Department of Energy (DOE) under Contracts No. DE-AC02-05CH11231 and No. DE-SC0013607, the DOE Office of Nuclear Physics under Contract No. DE-SC0011090, and the DOE Office of High Energy Physics under Contract No. DE-SC0012567. Cloud computing resources were provided through a Microsoft Azure for Research award. Additional support was provided by the Harvard Data Science Initiative.

---


