Mapping Machine-Learned Physics into a Human-Readable Space

Taylor Faucett,1 Jesse Thaler,2,3 and Daniel Whiteson1

1Department of Physics and Astronomy, UC Irvine, Irvine, CA 92627
2Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139
3The NSF AI Institute for Artificial Intelligence and Fundamental Interactions
(Dated: October 26, 2020)

We present a technique for translating a black-box machine-learned classifier operating on a high-dimensional input space into a small set of human-interpretable observables that can be combined to make the same classification decisions. We iteratively select these observables from a large space of high-level discriminants by finding those with the highest decision similarity relative to the black box, quantified via a metric we introduce that evaluates the relative ordering of pairs of inputs. Successive iterations focus only on the subset of input pairs that are misordered by the current set of observables. This method enables simplification of the machine-learning strategy, interpretation of the results in terms of well-understood physical concepts, validation of the physical model, and the potential for new insights into the nature of the problem itself. As a demonstration, we apply our approach to the benchmark task of jet classification in collider physics, where a convolutional neural network acting on calorimeter jet images outperforms a set of six well-known jet substructure observables. Our method maps the convolutional neural network into a set of observables called energy flow polynomials, and it closes the performance gap by identifying a class of observables with an interesting physical interpretation that has been previously overlooked in the jet substructure literature.

CONTENTS

I. Introduction 1
II. Translating from Machine to Human 3
   A. Average Decision Ordering 3
   B. Black-Box Guided Search Strategy 4
III. A Case Study in Jet Substructure 5
   A. Boosted Boson Classification 6
   B. Energy Flow Polynomials 7
IV. Supplementing Existing Observables 8
   A. Black-Box Guiding 9
   B. Physics Interpretation 10
V. Iteratively Mapping from Minimal Features 11
   A. Black-Box Guiding 11
   B. Comparison to Brute Force Search 13
   C. Comparison to Truth-Label Guiding 14
   D. Physics Interpretation 14
VI. Discussion 15
Acknowledgments 16

I. INTRODUCTION

It is widely appreciated that neural networks (NNs) and related machine learning (ML) tools can provide powerful solutions to important and difficult problems in high-energy physics [1, 2]. Examples of tasks that have benefitted from NNs include triggering [3], event reconstruction [4, 5], object identification [6–8], and event selection [9–11]. In all of these contexts, though, the physicist wonders: what has the machine learned? Satisfaction with improved performance is tempered by frustration with the “black-box” nature of ML strategies.

The advent of deep learning has made this question more urgent, as the data dimensionality of the tasks has increased dramatically and ML approaches have outperformed human-engineered strategies for problems that, until recently, were deemed too difficult for ML. Examples include event classification [12–17], jet substructure studies [18–22], jet flavor classification [23–27], detector unfolding [28–30], and uncertainty estimation [31–33]. In each case, a deep NN has successfully utilized more information from the high-dimensional low-level input data than was captured by a smaller number of physics-motivated high-level (HL) observables. When there is a performance gap between machine-learned and human-engineered strategies, physicists want to understand how the NN is using the low-level information to improve its performance. This desire also applies to situations where performance of the ML solution matches (but does not exceed) the human-engineered approach. Has the machine learned the same strategy that humans devised, or has it found an alternative solution with equal efficacy?

In this paper, we present a technique for translating a black-box ML strategy based on low-level inputs into a human-readable space of HL observables. Instead of trying to directly interpret a NN classifier, our approach is to use the NN as a guide for the construction of a simpler classifier which makes the same decisions but relies on a small number of physics-inspired, human-interpretable
inputs, selected iteratively from a large space of observables. As a demonstration of our method, we present a case study in jet classification [20], using a convolutional neural network (CNN) to guide the selection of a small set of HL observables called energy flow polynomials (EFPs) [34]. We find that the final set of HL observables provides the same classification performance as the CNN acting on the low-level inputs, but in a more compact, interpretable, and physically meaningful format. Our study suggests that physicists should consider an overlooked set of HL observables that are relevant to jet substructure classification.

This desire to gain insight into the nature of ML strategies is important on several levels. First, it is critical that information used by the NNs be validated as real and physical, rather than an artifact of the training samples or procedure. Even in cases where the ML training does not rely on simulated samples [35–37], it is important to understand what information is being used. Translating a black-box ML strategy into a simpler network that relies on smaller number of physically meaningful observables allows for effective validation. Second, having an interpretable strategy based on HL inputs allows for more reliable estimates of systematic uncertainties. If the HL space is small enough, the HL inputs themselves can be individually studied and calibrated, which is a more straightforward task than handling low-level inputs directly. Third, if one can replace a sophisticated ML strategy with a simpler network based on preprocessed inputs, this can enable faster interference and lower memory requirements at run-time [38–39]. Finally, if previously overlooked information in the low-level data is physical, identifying it can provide new insights into the nature of the problem. Indeed, in our jet classification case study, we show how the six HL observables studied in Ref. [20] can be augmented by a seventh HL observable that had not been previously considered in the literature. By scrutinizing the structure of the EFPs, we can provide a physical interpretation for this new observable.

There have been previous proposed strategies to draw connections between a learned NN strategy and existing HL observables. This can be done by comparing the performance with and without the HL observables [40] or projecting the decision surfaces along those observables [42]. An alternative strategy is to expand the NN function in a basis of the input features [43–45]. These strategies are valuable, but are primarily limited to studying the structure of the NN in terms of already-identified HL observables. The goal of the present work is to identify new HL observables relevant for ML tasks, starting from a large space of HL observables that is as broad and comprehensive as possible (yet still interpretable) and systematically mapping a black-box ML strategy into that space.

Our mapping strategy suggests a new approach to the application of deep learning to high-energy physics data. In this approach, training a powerful DNN on low-level inputs is just the first step, which helps gauge the effective upper limit on possible ML performance and determine asymptotically optimal decision boundaries. The new second step is translating as much of the ML strategy as possible to a well understood set of HL observables. This allows for physical interpretation of the information being used, validation of the modeling, definition of reasonable systematic uncertainties, as well as computational benefits due to dimensionality reduction.

An extended outline of this paper is as follows. In Sec. III we present a general approach to map a ML model's learned solution into a human-readable space. This mapping requires that we construct a large space of candidate HL observables and use a reliable similarity metric for comparing these observables to the learned solution. As our similarity metric, we introduce average decision ordering (ADO), which is related to Kendall’s rank correlation coefficient [44] and quantifies to what extent two classifiers make the same (even if incorrect) decisions. We then present a mapping strategy that leverages the ADO. Our black-box guided strategy iteratively finds the maximum ADO between the HL observables and a fixed black-box ML algorithm.

In Sec. IV we review the collider task of discriminating between jets originating from boosted W bosons and those originating from light quarks and gluons. This is a well-studied problem in the field of jet substructure [21–25], where both HL [26–28] and NN strategies [18–20] have proven effective. Our starting point will be the analysis of Ref. [20], which found a small but persistent improvement in classification performance with a deeply-connected CNN when compared to boosted decision tree (BDT) of HL observables. To augment the set of HL observables for jet tagging, we search the space of EFPs [34], which form an (over)complete basis of collider observables that are infrared and collinear (IRC) safe. We also introduce EFP variants inspired by IRC-unsafe observables that have been successful in other jet tagging studies [53–56].

The results of our case study are presented in Secs. V and VI. We start with the six HL observables from Ref. [20], and use the black-box guided strategy to identify a seventh HL observable that closes the performance gap with the CNN. We then apply the black-box guided strategy starting from just the mass and transverse momentum of the jet, comparing the results to a brute force strategy of directly searching the space of EFPs and a guided search based on ground truth labels. The black-box guided strategy significantly outperforms the label guided search, reaching comparable performance to the brute force strategy with considerably reduced computational costs. At the end of each of these sections, we provide a physical interpretation of the translated ML strategy, and we draw broader conclusions in Sec. VII.
II. TRANSLATING FROM MACHINE TO HUMAN

In our mapping approach, we seek to identify a small set of physically-motivated HL observables that, when combined into a joint classifier, make the same classification decisions as a deep network operating on the low-level features. Crucially, our set of HL features is designed to, when combined, maximize the classification performance by following the learned strategy of the black-box NN, which we argue below is more efficient than training directly on ground truth information. If this translation is successful, then we will have expressed the ML strategy more simply and transparently in terms of a few HL observables.

The first step in our approach is to identify a comprehensive set of HL observables that are potentially relevant for solving the ML task at hand. This in turn requires (human) knowledge about the physical system being studied and about the kinds of HL observables that have interpretable meaning. We know of no way to automate this step, though automation may not be desirable, as the choice and structure of the HL observable space defines the physical interpretation. For our jet substructure classification case study, the EFPs have already been identified as a suitable basis of HL observables [34], as discussed further in Sec. III E. Other ML tasks in high-energy physics might require the development of alternative bases of HL observables.

In the rest of this section, we describe the aspects of our approach that are generic to any ML task, focusing on the case of binary classification. To evaluate the relative performance of our simple HL network and a black-box NN, we need a metric to evaluate whether two classifiers make the same classification decisions. There are many such metrics one could use, but we introduce ADO, in part because it shares the conceptual simplicity of the area under the curve (AUC) metric often used to benchmark classifiers against ground truth. Armed with an exploratory set of HL observables and a metric for assessing learning similarity, we then present a guiding strategy to map black-box NNs into a physically meaningful space.

A. Average Decision Ordering

Our guided strategy requires a similarity metric that compares the output of two decision functions \( f(x) \) and \( g(x) \). Here, \( x \) represents the full high-dimensional low-level data, which are inputs to both the black-box NN and the physically-motivated HL observables. Of course, the definition of similarity must reflect the task for which these decision functions are applied, which in this case is binary classification. Because classification performance is invariant under any non-linear monotonic transformation of \( f \) or \( g \), our similarity metric cannot be affected by such a transformation. This rules out naive metrics like functional overlap or linear correlation.

Furthermore, it is not sufficient to simply compare the overall performance of two classifiers over a given dataset, since that does not provide information about how the low-level inputs are being used. As discussed in Ref. [35], two decision functions might use information from different regions of the low-level input space and make conflicting classification decisions case by case, yet still achieve similar overall performance. The key to our guided strategies is that we aim to match not just the classification performance of the black-box NN, but also the specific classification decisions.

We assume that the decision functions \( f(x) \) and \( g(x) \) are real valued and that the final binary classification is determined by a threshold on the decision function output. Objects on one side of the threshold are labeled “signal”, while objects on the other side are labeled “background”. Depending on the particular application, this threshold can be tuned to different points on the receiver operating characteristic (ROC) curve to optimize the signal acceptance versus background rejection. To quantify overall classification performance, we use the AUC, which is equivalent to the probability that a randomly selected signal/background pair is correctly ordered by a decision function \( f(x) \):

\[
\text{AUC}[f] = \int \text{dx} \text{dx'} p_{\text{sig}}(x) p_{\text{bkg}}(x') \Theta(f(x) - f(x')).
\]

Here, \( \Theta \) is the Heaviside theta function (i.e. \( \Theta(x < 0) = 0 \) and \( \Theta(x \geq 0) = 1 \)) and \( p_{\text{sig}} \) and \( p_{\text{bkg}} \) are the ground truth signal and background probability distributions. A perfect decision function has AUC = 1 and random guessing yields AUC = \( \frac{1}{2} \).

To compare the classification behavior of two decision functions, we consider the decision surface defined by a threshold on the function output. For each function, the set of such thresholds defines a set of surfaces in \( x \) space. If two decision functions have the same decision surfaces, then they are effectively using the same low-level information for classification. Note that the absolute output values of the decision functions are not relevant for determining whether the decision surfaces are similar. The relative locations of the decision surfaces are determined by the relative ordering of the two decision functions when evaluated at pairs of points in the input space. We can encapsulate this information via the decision ordering (DO) for a pair of points \( x \) and \( x' \):

\[
\text{DO}[f,g](x,x') = \Theta\left((f(x) - f(x'))(g(x) - g(x'))\right),
\]

where 1 corresponds to \( f \) and \( g \) having the same ordering and 0 corresponds to inverted ordering.

If two decision functions have DO = 1 for all pairs of \( x \) and \( x' \), then they are monotonically related to each other, have identical decision surfaces, and are therefore identical for the purposes of classification. To build a summary statistic, we average over all possible values of \( x \) and \( x' \), weighted by the signal and background distri-
butions, yielding the ADO:

\[ \text{ADO}[f, g] = \int \! dx \, dx' \, p_{\text{sig}}(x) \, p_{\text{bkg}}(x') \, \text{DO}[f, g](x, x'). \]  

(3)

This evaluates to 1 if the decision functions make the same relative classification decision for every pair, to 0 if the functions make the opposite classification for every pair, and to 1/2 if there is no consistency in their orderings. Since a decision function can be trivially inverted, the case of ADO = 0 and ADO = 1 have the same meaning, so we map \( \text{ADO} \rightarrow 1 - \text{ADO} \) whenever it is less than 1/2. The ADO has a similar philosophy to Kendall's rank correlation coefficient [44], with the key difference that we are comparing inputs drawn from separate signal and background distributions.

To gain intuition for the ADO, note that it has a very similar structure to the AUC in Eq. (1). The AUC is the probability that a single decision function orders objects correctly relative to ground truth. The ADO is the probability that two decision functions order objects in the same way, even if incorrectly. In the case that \( f(x) = p_{\text{sig}}(x)/p_{\text{bkg}}(x) \) is the likelihood ratio, then \( f(x) \) is an optimal classifier by the Neyman-Pearson lemma, so an ADO = 1 implies that \( g(x) \) defines the same optimal decision boundaries as \( f(x) \). In most ML applications, one is trying to maximize the AUC or other similar metric of absolute classification performance. Our guided strategies, by contrast, aim to maximize the ADO relative to an already trained ML tool.

There are other similarity metrics that one could use, but they are not as easy to interpret in terms of classification decisions. One way to capture information similarity is to use mutual information, or more appropriately to binary classification, mutual information with the truth [65]. For our guided strategies, though, we are less interested in whether two decision functions have the same quantity of information available to a classification task, and more interested in quantifying the degree to which two decision functions make classification decisions in the same way. Even if \( f(x) \) and \( g(x) \) contain a high level of mutual information, they do not necessarily define the same decision boundaries. This is especially important to keep in mind given the flexibility of deep networks, which allow the same discrimination power to be encoded in many informationally equivalent ways. Beyond the ADO, there are other summary statistics one could use based on the raw DO information, and we leave a study of those alternatives to future work.

B. Black-Box Guided Search Strategy

The idea behind the black-box guided strategy is shown in Fig. 1 where the goal is to find HL observables that maximize the ADO relative to an already trained ML tool. We denote the reference black-box network as “BBN” (with apologies to cosmologists), and it will typically be some kind of deep network acting on the low-level inputs. Starting from a large set \( S \) of human-defined HL observables motivated by physics considerations, our aim is to build a high-level network (HLN) with the same decision surfaces as the BBN. The initial step \((n = 0)\) in the black-box guided approach is to identify the observable \( \text{HL}_1 \) that has the largest ADO with the BBN:

\[ \text{HL}_1 = \arg\max_{\text{HL}_1 \in S} \text{ADO}[\text{BBN}, \text{HL}_1]. \]  

(4)

Here, the \( X_{\text{all}} \) subscript indicates that we are using the full set of signal/background training pairs \((x, x')\) when computing the ADO. The observable \( \text{HL}_1 \) is therefore the physics-motivated observable in the set \( S \) that best approximates the decision surfaces of the black box.

In the next step \((n = 1)\), we focus our search for HL observables in regions of the feature space where the black-box network disagrees with our current set of HL observables already identified in the previous steps into a joint network:

\[ \text{HL}_{n+1} = \text{NN}[\text{HL}_1, \ldots, \text{HL}_n], \]  

(7)

where NN indicates a neural network trained on the full set of signal/background training pairs \((x', x')\) when computing the ADO. The observable \( \text{HL}_{n+1} \) is therefore the optimal classifier by the Neyman-Pearson lemma, so an ADO = 1 implies that \( g(x) \) defines the same optimal decision boundaries as \( f(x) \). In most ML applications, one is trying to maximize the AUC or other similar metric of absolute classification performance. Our guided strategies, by contrast, aim to maximize the ADO relative to an already trained ML tool.

There are other similarity metrics that one could use, but they are not as easy to interpret in terms of classification decisions. One way to capture information similarity is to use mutual information, or more appropriately to binary classification, mutual information with the truth [65]. For our guided strategies, though, we are less interested in whether two decision functions have the same quantity of information available to a classification task, and more interested in quantifying the degree to which two decision functions make classification decisions in the same way. Even if \( f(x) \) and \( g(x) \) contain a high level of mutual information, they do not necessarily define the same decision boundaries. This is especially important to keep in mind given the flexibility of deep networks, which allow the same discrimination power to be encoded in many informationally equivalent ways. Beyond the ADO, there are other summary statistics one could use based on the raw DO information, and we leave a study of those alternatives to future work.
emphasizing that the ADO, or some other metric for network decision similarity, is essential for this approach to work.

Later in Sec. V C we will compare this black-box guided approach to a label guided approach. Instead of using the ADO, the label guided approach uses the AUC with respect to ground truth information. It is straightforward to understand why the ADO is superior to the AUC for guiding purposes. To the extent that the BBN is well trained, it represents a good approximation to the Neyman-Pearson optimal classifier. Achieving the correct DO relative to the optimal classifier for every signal/background training pair is the best one could ever hope to do. Therefore, if the black-box guiding strategy is working correctly, then the subsets $X_n$ will get smaller and smaller until almost all signal/background pairs have been correctly ordered relative to the BBN.

By contrast, the AUC captures DO relative to truth labels. Unless the BBN is able to achieve AUC $= 1$, there will inevitably be signal/background pairs that are incorrectly ordered even by the theoretically optimal classifier. Instead of getting smaller and smaller, the subsets $X_n$ will stall at the set of signal/background pairs that can never be ordered correctly. This in turn means that the classification performance of HLN$_n$ will stall well below the theoretical maximum in the label guided approach. That is why we advocate for the selection of HL observables to be guided by the ADO, since then the classification performance of the HLN$_n$ will eventually match that of the BBN, as desired.

As with any “greedy algorithm”, our black-box guided strategy cannot identify situations where two HL observables could be combined simultaneously to match the BBN decision surfaces. This means that we might miss sets of observables that are individually poor classifiers but perform well jointly. If the goal were to just to maximize performance, this would be an undesirable feature. In the context of mapping a black-box ML strategy to a physically-interpretable space, though, we are indeed looking for individual observables with high information content relevant for classification, so this greedy strategy is the one most likely to yield physical insight.

### III. A CASE STUDY IN JET SUBSTRUCTURE

We now apply the technique introduced in Sec. II to a specific case study involving jet classification at the LHC. In this section, we review boosted $W$ boson classification using jet substructure and highlight the elements of Ref. [20] that will be used in our case study. We then introduce the EFPs [34] as our set of HL physics-motivated observables. Details about our NN architectures and training parameters are provided in App. [A].
A. Boosted Boson Classification

Massive objects produced at the LHC often have enough transverse momentum that their decay products become collimated. For an object with a hadronic decay mode, such as a W boson decaying to a quark-antiquark pair ($W \rightarrow q\bar{q}'$), the resulting jet in the detector consists of two clusters of energy, one from each of the fragmenting quarks. The substructure of these jets is distinct from those that arise from the fragmentations of a single hard quark or gluon. Identification of jets with nontrivial substructure has become an essential tool for probing the nature of collisions at the LHC [21, 40, 50].

There are many different ways to represent the information in a jet. At the most fundamental level, a jet is a variable-length collection of four-vectors with associated particle properties, motivating set-based ML tools [69, 74]. Another popular approach is to describe a jet as a grid of calorimeter cells with energy depositions, giving rise to a “jet image” [19, 72]. In any of these low-level representations, the jet data is high dimensional. This motivates the development of HL observables that intelligently summarize the low-level information to reduce the effective dimensionality of the task. Physicists have engineered numerous HL observables tasks that incorporate domain knowledge about jet formation (see Refs. [49, 57–62, 76, 83] for an incomplete list). Typical usage is to apply cuts on one or more of these HL observables, or to combine several of them using a shallow ML classifier.

In the context of jet classification, ML tools based on low-level inputs have outperformed traditional strategies based on HL observables [51]. Of course, the HL observables themselves are just function of the low-level inputs, so it should be possible to find a large enough set of physics-motivated HL observables that can match the performance of these ML classifiers [55, 87]. This is indeed the intuition behind the guided strategy in Sec. [11] where the goal is to leverage a black-box ML method to identify the most effective HL observables.

Our case study is based on the same datasets as Ref. [20]. These datasets correspond to $\sqrt{s} = 14$ TeV proton-proton collision, where hard scattering and resonance decay were generated using MadGraph 5 v2.2.3 [58], showering and hadronization were generated with Pythia v6.426 [89], and the response of the detectors was simulated with Delphes v3.2.0 [90]. The boosted W signal process is diboson production ($pp \rightarrow W^+W^-$), which yields two fat jets each with 2-prong substructure. The background process is QCD dijet production ($pp \rightarrow qg, gg, gq$), which typically yields 1-prong jets. These samples do not include contamination from pileup (multiple proton-proton collision per beam crossing). Jets are clustered using the anti-$k_t$ algorithm [91] with radius parameter $R = 1.2$, using FastJet 3.1.2 [92]. The dataset contains $5 \times 10^6$ events, split equally between signal and background. Following the approach in Ref. [20], each jet is pixelated into a $32 \times 32$ grid in the rapidity-azimuth plane, and a jet image is formed from the transverse momentum ($p_T$) deposits in each cell. The jet image is then trimmed [93], where subjets of radius $R_{sub} = 0.2$ are discarded if their $p_T$ is less than 3% of the original jet. The final jet selection takes jets with trimmed momentum $p_T^{\text{trimmed}} \in [300, 400]$ GeV within the rapidity range $|\eta| < 5.0$. While important jet information is lost by pixelation and trimming, we include these steps in our analysis in order to perform an apples-to-apples comparison to Ref. [20].

The trimmed jet’s constituents are used to compute six HL jet substructure observables: the trimmed jet mass ($M_{jet}$), four ratios of energy correlation functions ($C_{\beta=1}^2$, $C_{\beta=2}^2$, $D_{\beta=1}^2$, $D_{\beta=2}^2$) [60, 62], and the $N$-subjettiness ratio ($\tau_2^\beta$) [55, 29]. These observables are well-established in the context of boosted $W$ classification, including studies at ATLAS [94, 95] and CMS [96]. The $W$ boson classification performance of these six HL observables is summarized in Table I. The trimmed jet mass is the most powerful single observable, while the 80.4 GeV mass peak is a characteristic feature of boosted $W$ bosons.

We can use the ADO from Eq. (3) to gain additional insight into these six HL observables. In Fig. 2 we assess the pairwise ADO between each of the HL observables considered. The observable pairs that make the most similar decisions (i.e. ADO $\rightarrow 1$) are $C_{\beta=1}$ with $C_{\beta=2}$ and $D_{\beta=1}^2$ with $D_{\beta=2}^2$. This is expected since these observables have relatively similar structures except for the choice of $\beta$ coefficient, which controls the weighting of angular information within the jets. These pairs also have similar AUC values, as seen in Table I, since pairs that make common classification decisions should exhibit similar AUC values, as seen in Table I, since pairs that make common classification decisions should exhibit similar ADO (ADO) to the benchmark CNN is also shown. Details of the NN architectures are provided in App. A.

| Observable | AUC | ADO(CNN, Obs.) |
|------------|-----|----------------|
| $M_{jet}$  | 0.898 ± 0.004 | 0.807 |
| $C_{\beta=1}^2$ | 0.660 ± 0.006 | 0.584 |
| $C_{\beta=2}^2$ | 0.604 ± 0.007 | 0.548 |
| $D_{\beta=1}^2$ | 0.790 ± 0.005 | 0.743 |
| $D_{\beta=2}^2$ | 0.807 ± 0.005 | 0.762 |
| $\tau_2^\beta$ | 0.662 ± 0.006 | 0.600 |
| 6HL        | 0.9504 ± 0.0002 | 0.971 |
| CNN        | 0.9531 ± 0.0002 | 1.000 |
| 7HLblack-box | 0.9528 ± 0.0003 | 0.971 |

TABLE I. Classification performance of the six HL observables studied in Ref. [20], as well as a 6HL joint classifier. The six HL observables face a small but significant performance gap compared to the benchmark CNN. As discussed later in Sec. [V A], this performance gap is bridged by a seventh feature discovered using our black-box guided strategy. The uncertainty on the AUC is computed from 1 standard deviation of 10-fold cross-validation. The decision similarity (ADO) to the benchmark CNN is also shown. Details of the NN architectures are provided in App. A.
sions (i.e. \( \text{ADO} \to \frac{1}{2} \)) are \( M_{\text{jet}} \) with \( C^{\beta=1}_2 \) and \( C^{\beta=2}_2 \) with \( D^2_2 \). For \( M_{\text{jet}} \) versus \( \tau^{\beta=1}_{21} \), this is expected since \( N \)-subjettiness probes the degree of prong-like collimation, whereas mass is sensitive to the energies of the prongs and their relative angle. For \( C^{\beta=2}_2 \) versus \( D^2_2 \), this is expected since they have different scalings under boosts along the jet direction \([62]\). Pairs that make dissimilar decisions can often be combined into more powerful joint classifiers. This is shown in Fig. 3 where we consider the pairwise classifiers \( \text{NN}[\text{HL}_i, \text{HL}_j] \), where the details of the \( \text{NN} \) parameters are presented in App. A.2. More comprehensive studies of these six jet substructure observables can be found in Ref. \([34]\).

While these six engineered HL features are powerful jet substructure discriminants, they do not capture the full information relevant for \( W \) boson tagging. Viewing the calorimeter cells as pixels of a two-dimensional image, we can try to enhance the discrimination power using computer vision techniques \([18, 20, 22, 27, 32, 75, 97, 98]\). Indeed, Ref. \([20]\) demonstrated that a deeply connected CNN using the low-level jet image inputs yielded better classification performance than the six HL observables combined with a BDT. The performance gain was modest though persistent, making it an excellent benchmark problem for studying the interpretation of ML strategies. We repeat this exercise in Table I, now using the \( \text{NN} \) parameters in App. A for the CNN and for the 6HL combination:

\[
6\text{HL} \equiv \text{NN}[M_{\text{jet}}, C^{\beta=1}_2, C^{\beta=2}_2, D^2_2, D^{\beta=2}_2, \tau^{\beta=1}_{21}],
\]

where we find a 0.0027 ± 0.0003 gap in AUC, as seen in Table I. Using our guided strategy, we seek to understand the nature of this performance gap, and whether the CNN has found a strategy similar to the existing HL observables or something distinct. Does the gap indicate a mild optimization of the same basic HL ideas, or does it hint at the existence of a new HL observable not appearing previously in the jet substructure literature?

### B. Energy Flow Polynomials

In order to map the CNN from Ref. \([20]\) to a human-readable space, we first define a suitable set of physics-motivated HL observables for use in the guided strategies. This requires domain knowledge about the underlying physics as well as intuition for the kinds of information that might be missing from existing HL observables. This also requires identifying HL observables that are likely to work well as classifiers individually, since the black-box guided strategy in Sec. II B is based on finding a single observable that maximizes the ADO in each step.

Our set of HL observables is based on the EFPs \([34]\). The EFPs are a large (formally infinite) set of parametrized engineered functions, inspired by previous work on energy correlation functions \([60, 62, 99–102]\). In the jet image representation, they are defined in terms of the momentum fraction \( z_a \) of calorimeter cell \( a \), as well as the pairwise angular distance \( \theta_{ab} \) between cells \( a \) and \( b \). The EFPs are built in increasing levels of complexity, from simple sums over single cells to many higher-order combinations of momentum and pair-wise angles. An EFP can be represented as a multigraph where:

\[
\text{each node} \implies \sum_{a=1}^{N} z_a, \quad (11)
\]

\[
\text{each } k\text{-fold edge} \implies (\theta_{ab})^k. \quad (12)
\]
As one example, we have:

$$z_a^{(κ)} = \frac{p_T a}{\sum_b p_T b}^κ, \quad θ_{ab}^{(β)} = \left(Δφ_{ab}^2 + Δθ_{ab}^2\right)^{β/2}. \quad (13)$$

From these graph representations, we can express both connected and disconnected graphs. For the purposes of our study, we only consider connected graphs.

The observable corresponding to each graph can be modified with parameters (κ, β). These parameters determine the specific meaning of z_a and θ_{ab}, where

$$z_a^{(κ)} = \frac{p_T a}{\sum_b p_T b}^κ, \quad θ_{ab}^{(β)} = \left(Δφ_{ab}^2 + Δθ_{ab}^2\right)^{β/2}. \quad (15)$$

Here, p_T a is the transverse momentum of cell a, and η_{ab} (φ_{ab}) is pseudorapidity (azimuth) difference between cells a and b. The original IRC-safe EFPs require κ = 1, however we include examples with κ ≠ 1 to explore a broader space of HL observables, motivated by Refs. [63–66].

Note that κ > 0 generically corresponds to IR-safe but C-unsafe observables. We intentionally include zero and negative values of κ to explore both IR-unsafe and C-unsafe observables as well. For our study, we use the ENERGYFLOW python package [103] to translate jet-image p_T, η, and φ information to EFPs with varying graphs and choices of κ and β.

For our guided search, we consider all combinations of (κ, β) where κ = [-1, 0, 1/2, 1, 2] and β = [1/2, 1, 2]. Each of the 15 combinations of (κ, β) are applied to the complete set of connected graphs with degree (i.e. number of edges) d ≤ 7 along with all connected graphs with degree d ≤ 8 and chromatic number c = 4 (to be defined in Sec. IVB below), which comes to 509 in total. This yields a space of 7,635 HL observables to search from. Note that β in Eq. (15) can sometimes be traded for k in Eq. (12); we remove degenerate graphs from our space, reducing our pool of unique observables to 7,545.

It is important to emphasize that, although the EFP space constitutes a formally complete basis for (IRC-safe) jet classification, we are primarily concerned with the pragmatics of isolating individual observables that can map out the CNN behavior. The ideal case is that the CNN strategy maps to a single EFP, indicating that it can be expressed compactly in terms that can be easily interpreted by humans. Failing that, though, it is still of considerable value if a similar mapping can be made using a small collection of observables [85, 87]. This would still provide a significantly more physically meaningful interpretation of the data and a marked reduction in data complexity and dimensionality.

Beyond this specific benchmark example, if one is unable to map the CNN strategy into a small number of EFPs, this could mean one of two things. First, it could mean that the CNN strategy simply does not operate in this HL space, requiring us to revisit the assumption that the HL space was sufficiently complete to capture the essential information for jet classification. Second, it could mean that the CNN strategy is still encodable in terms of these HL observables, but in a more complex combination. As an example of this second possibility, consider the C_2 [60] and D_2 [62] observed discussed in Sec. IIIA. These can be written as EFPs with κ = 1:

$$C_2^{(β)} = \frac{1}{\left(\theta^2\right)^{2}}, \quad (16)$$

$$D_2^{(β)} = \frac{1}{\left(\theta^3\right)^{3}}, \quad (17)$$

where the graphs corresponds to:

$$= \sum_{a=1}^{N} \sum_{b=1}^{N} \sum_{c=1}^{N} z_a z_b z_c \theta_{bc}^{(β)} \theta_{ca}^{(β)} \theta_{ab}^{(β)}. \quad (18)$$

The guided strategies, however, would not necessarily be able to identify these ratio combinations unless they were defined ahead of time. Therefore, whether or not the guided mapping is effective, one learns something about the nature of the physics problem either way.

IV. SUPPLEMENTING EXISTING OBSERVABLES

In this section, we demonstrate the success of the mapping strategy from Sec. III in searching for an additional HL observable in the context of boosted W classification.

From Table II we saw that the difference in classification power between a CNN acting on jet images and a NN combination of six HL observables is relatively small, but genuine and statistically significant. As such, it is interesting to ask whether this existing set of six HL observables could be supplemented by a new single HL observable which has not yet been considered by human physicists. We employ our black-box guiding strategy to find such a seventh HL observable, which closes the performance gap previously identified in Ref. [20].

---

1 We thank Patrick Komiske and Eric Metodiev for discussions related to the normalization of the κ ≠ 1 EFPs.

2 For κ < 0, empty cells are omitted from the sum in Eq. (11). This is not as discontinuous as one might naively think due to the pixelation and trimming steps.

3 It might be interesting to combine the guided strategy with some kind of symbolic regression to find interesting combinations [104]. If this symbolic regression allowed for index contraction, then one could use the energy flow moments [105] to more efficiently search the space of β = 2 EFPs.
A. Black-Box Guiding

The first step of the black-box guided strategy from Sec. II.B is to identify the subset of signal/background pairs that are differently ordered by the CNN and the 6HL combination:

\[ X_6 = \{(x, x') | \text{DO}[\text{CNN}, 6\text{HL}](x, x') = 0\}. \quad (20) \]

Though we have \(6.25 \times 10^{12}\) signal/background pairs, we construct \(X_6\) from a randomly selected subset of \(5 \times 10^7\) pairs. We then search for the EFP that has the greatest decision similarity to the CNN in the \(X_6\) subspace, which ideally captures all of the remaining discrepancies between the CNN and 6HL approaches:

\[ \text{HI}_7^{\text{black-box}} = \arg\max_{\text{HL} \in \text{EFPs}} \text{ADO}[\text{CNN}, \text{HL}]_{X_6}. \quad (21) \]

The results are shown in the first row of Table III. The EFP with the largest ADO with the CNN in the \(X_6\) subspace is:

\[ \langle \kappa = 2, \beta = \frac{1}{2} \rangle = \sum_{a=1}^{N} \sum_{b=1}^{N} \sum_{c=1}^{N} \sum_{d=1}^{N} s_{a-b}^2 s_{c-d}^2 \sqrt{\theta_{ab} \theta_{cd} \theta_{ad} \theta_{bc}}. \quad (22) \]

By itself, Eq. (22) only has an AUC of 0.8031, but when used as the seventh feature of a NN that also uses the previously identified 6HL observables,

\[ \text{7HL}_{\text{black-box}} \equiv \text{NN} \left[ M_{\text{jet}}, \ldots, \tau^2_{\beta=1}, \langle \kappa = 2, \beta = \frac{1}{2} \rangle \right], \quad (23) \]

it closes the performance gap with the CNN by achieving AUC = 0.9528 \(\pm 0.0003\), as previewed in Table I. Interestingly, this happens even though the ADO between the CNN and 7HL_{black-box} is only 0.971, implying that they still make inconsistent decisions around 3% of the time. So while the black box has guided the selection of a new HL observable that closes the AUC performance gap, the remaining ADO gap implies that there is additional information not being captured.

The remaining rows of Table III show portions of the ranked list of 7,545 EFPs, ordered by their ADO values. Note that the statistical uncertainties on the ADO are large enough that the precise ranking is not so meaningful, though the overall trends are. One striking feature is that many observables have similar ADO to Eq. (22), and they often feature \(\kappa = 2\) and \(\beta = \frac{1}{2}\). Recall that \(\kappa = 2\) corresponds to IRC-unsafe EFPs, which suggests that IRC-unsafe information is valuable (though perhaps not uniquely so) for mapping the CNN strategy. Similarly, the appearance of \(\beta = \frac{1}{2}\) suggests the importance of probing small-angle behavior. Other IRC-unsafe EFPs with \(\kappa = 0\) and \(\kappa = -1\) also perform well, especially the constituent multiplicity appearing third on this list. The best performing IRC-safe \(\kappa = 1\) observable appears 5531th in this list and is not able to close the performance gap with the CNN. Specifically, the EFPs in Eqs. (18) and (19) with \(\kappa = 1\) have relatively small ADO in the \(X_6\) subspace, never getting above 0.5279. This is as one might expect, since these observables already effectively appear in the \(C_2\) and \(D_2\) combinations. Further discussions of the physics implications are provided below.

For completeness, we show distributions for the top three EFPs from Table III in Fig. 4, both in the full space as well as in \(X_6\). The first two observables show good separation between signal and background in the full space, as expected given that their AUC is around 0.8. The third observable, constituent multiplicity, is a relatively poor discriminant by itself. When restricted to the \(X_6\) subspace, there is only modest residual separation power shown by these three observables, but enough to close the performance gap with the CNN.
TABLE II. A selection of EFPs, sorted by their similarity with the CNN, evaluated using ADO in the differently-ordered subspace $X_6$. This corresponds to one step in the black-box guiding technique depicted in Fig. 1. After the top 10, EFPs are shown if they correspond to a dot graph, appear in the $C_2/D_2$ observables from Eqs. (16) and (17), or have the highest ADO among graphs with a given value of $\kappa$, $\beta$, or chromatic number.

### B. Physics Interpretation

Our first physics conclusion is that the $\kappa$-augmented EFPs space is sufficiently comprehensive to close the performance gap between the 6HL and the CNN. Had we restricted our attention to just the IRC-safe EFPs, this would not have been the case, since the top ranked $\kappa = 1$ EFP in both strategies can only achieve $\text{AUC} = 0.9507$ when combined with the six previous HL observables. Thus, IRC-unsafe information seems essential for closing the performance gap.

Fascinatingly, $\kappa = 2$ appears prominently in the top ten EFPs, though in a different form than previously considered in the literature. The key feature of the $\kappa = 2$ EFPs is that they weight higher energy particles more
than lower energy particles. Looking at the top $\kappa = 2$ observables in Table I, they all have the common feature of corresponding to chromatic number $c = 3$ graphs. Chromatic number is the minimum number of colors needed to decorate the nodes of a graph such that no edge connects same-color nodes. If an EFP has chromatic number $c$, then it is only non-zero if the jet has at least $c$ distinct particle directions, making it an effective probe for deviations from $(c-1)$-prong substructure. The $\kappa = 2$ and $c = 3$ EFPs found by our guided strategy therefore probe IRC-unsafe deviations from 2-prong substructure (as one might expect for boosted $W$ tagging), with a particular emphasis on the higher energy particles inside the jet.

By contrast, the only $\kappa = 2$ observable that has received any significant attention in the jet substructure literature is $p_T^D$ [63, 64]. In the EFP language, $p_T^D$ is a $c = 1$ graph with no edges:

$$\cdot (\kappa=2) = \sum_{a=1}^{N} z_a^2. \quad (24)$$

Here, we see that $p_T^D$ is only ranked 5610th by ADO. Apparently, generic IRC-unsafe information is not, by itself, useful for boosted $W$ boson classification, but must be paired with the correct angular dependence to highlight the physics of interest. It is interesting that $\beta = \frac{1}{2}$ is preferred as the angular exponent, since this choice appeared previously in the context of the Les Houches angularity for quark/gluon discrimination [66].

There are also $\kappa = 0$ observables in the top ten EFPs, including the well known constituent multiplicity:

$$\cdot (\kappa=0) = \sum_{a=1}^{N} 1. \quad (25)$$

The fact that a $\kappa = 0$, $c = 1$ observable yields nearly the same performance as a class of $\kappa = 2$, $c = 3$ observables is a surprising result of our study. Our tentative interpretation is that this represents two complementary approaches to solving this jet classification task. On the one hand, boosted $W$ bosons are 2-prong objects, so one expects $c = 3$ observables to be most relevant. Indeed, the numerators of Eqs. (16) and (17) are $c = 3$ graphs that probe 2-prong substructure, which was part of the original motivation for the $C_2$ and $D_2$ observables. On the other hand, the background quark and gluon jets are 1-prong objects, and constituent multiplicity is well-known to be a powerful quark/gluon discriminant [66].

The next $\kappa = 0$ observable on the list has $c = 2$ and $\beta = \frac{1}{2}$, which is an IRC-unsafe probe of 1-prong substructure with an emphasis on collinear physics, which should also be an effective quark/gluon discriminant. This suggests that one can improve the classification performance either with a refined probe of the $W$ boson signal or a refined probe of the quark/gluon background, which happens to have a similar effect on the decision boundaries.

In summary, by translating an ML strategy into a human-readable space, we have identified an important class of jet substructure observables that have been missing from previous boosted $W$ boson studies. This motivates further studies of IRC-unsafe observables, especially high degree EFPs with $\kappa = 2$. In Sec. [VI] we discuss the implications of this result on future work with jet substructure observables.

V. ITERATIVELY MAPPING FROM MINIMAL FEATURES

In the previous section, our aim was to supplement an existing set of HL features with one new feature to bridge the gap with the CNN performance. This jet substructure case study is unusual, however, in that it benefits from a highly mature literature of theoretically motivated features. Other applications of our black-box guided strategy may have to begin from a more minimal starting point and build an HL classification strategy essentially from scratch.

In this section, we start from just the most basic jet properties—transverse momentum $p_T$ and jet mass $M_{jet}$—and iteratively identify a small set of EFPs relevant for boosted $W$ boson classification. Using the black-box guided strategy, we are able to match the CNN performance using around 7 EFPs. This is a similar dimensionality as the 7HL combination (which did not include $p_T$), though the physics features being probed will turn out to be interestingly different. We then show that this black-box strategy is more computationally efficient than a brute-force search and more effective than a label-guided search.

A. Black-Box Guiding

Here, we apply the same black-box approach as Sec. [VIA], starting just from the smaller set of observables, $p_T$ and $M_{jet}$. The motivation for this starting point is as follows. The $W$ boson mass at 80.4 GeV is one of the most important (and obvious) features of boosted $W$ bosons. Because of the choice of $z_a$ variable in Eq. (14), though, the EFPs are dimensionless. Therefore, we need at least one dimensionful HL observable to capture the $W$ boson mass peak, and either $p_T$ or $M_{jet}$ would suffice for this purpose.

We begin from both $p_T$ and $M_{jet}$ for two reasons. The first is that they are ubiquitous jet observables appearing in myriad collider studies. The second is to streamline the selection of EFPs. Naively, $M_{jet}$ could be derived from $p_T$ using the EFP in Eq. (15) with $\kappa = 1$ and $\beta = 2$:

$$\cdot (\kappa=1, \beta=2) \approx \frac{M_{jet}^2}{p_T^2}. \quad (26)$$

With the choice of $\theta_a$ variable in Eq. (15), though, Eq. (26) is only approximately true, so multiple EFPs
FIG. 5. Performance of the black-box guided search strategy to map the CNN solution into human-interpretable observables. Here, we start from just the basic jet features $p_T$ and $M_{\text{jet}}$ and iteratively add one EFP at a time. The performance is shown in terms of AUC (top) and ADO (bottom) as a function of the scan number. The performance of a brute-force scan of the EFP space (Sec. V B) and a truth-label guided search (Sec. V C) are also shown. For reference, the performance of the CNN and of the existing 6HL features are indicated by horizontal lines.

are needed to map out the mass information if $p_T$ is the only dimensionful scale. We checked that the black-box strategy is still effective starting from just $p_T$ or from just $M_{\text{jet}}$, but the chosen EFPs tend to be more mass-like in their structure. By contrast, starting from both $p_T$ and $M_{\text{jet}}$ yields more variation in the types of EFPs selected.

We start by training a NN on just the $p_T$ and $M_{\text{jet}}$ information:

$$\text{HLN}_0 \equiv \text{NN}[p_T, M_{\text{jet}}].$$

This yields an AUC of 0.9119, which is substantially below the CNN performance for boosted $W$ boson tagging. We then restrict our attention to the subset of events that are differently ordered by these minimal features relative to the CNN:

$$X_0 = \left\{ (x, x') \left| \text{DO}[\text{CNN}, \text{HLN}_0](x, x') = 0 \right. \right\}. \quad (28)$$

The ADO between the CNN and HLN_0 is 0.9150, so $X_0$ contains 8.5% of the original $X_{\text{all}}$ sample, though we only consider a random subset of $5 \times 10^7$ pairs in $X_0$ to reduce the computational burden. Our aim is to find a set of EFPs that can order these signal and background events the same as the CNN decision boundaries.

To identify the $n$-th EFP, we use the black-box guided strategy of Sec. II B, adapted to the current notation:

$$\text{EFP}_n = \arg\max_{\text{EFP} \in S} \text{ADO}[\text{CNN, EFP}|_{X_{n-1}}]. \quad (29)$$

We construct a new joint classifier that includes this EFP:

$$\text{HLN}_n \equiv \text{NN}[p_T, M_{\text{jet}}, \text{EFP}_1, \ldots, \text{EFP}_n]. \quad (30)$$

This allows us to identify the remaining differently-ordered subset of events:

$$X_n = \left\{ (x, x') \left| \text{DO}[\text{CNN}, \text{HLN}_n](x, x') = 0 \right. \right\}. \quad (31)$$

where in each iteration we only keep a random subset of $5 \times 10^7$ pairs. The main computational cost in this procedure is in training the joint classifier in Eq. (30).

The AUC and ADO values for this black-box guided procedure are shown in Fig. 5 versus EFP scan iteration, and in Fig. 6 versus cumulative computing time. More details about the selected EFPs are given in Table III. By the 5th iteration, the AUC performance matches that of the 6HL combination. By the 7th iteration, the AUC performance matches that of the CNN, with an ADO of nearly 0.975, indicating closer agreement with the CNN decisions than we found with the 7HL black-box strategy. Since we started from a minimal set of jet features, it...
is not surprising that the EFPs identified here are qualitatively different from the ones in Sec. IV. The physics interpretation of these various EFPs will be presented in Sec. V D.

### B. Comparison to Brute Force Search

An alternative approach to maximizing ADO is to perform a brute-force search through the space of EFPs to find the set that maximally matches the decisions of the CNN. This is much more computationally expensive than the black-box guided strategy, but it has the potential to converge to a smaller number of EFPs if there are important correlations between the observables. In an absolute brute force search, one would construct all possible sets of EFPs, and evaluate the ADO of each relative to the CNN; given the number of graphs and combinations, this would be completely intractable. Instead, we attempt an iterative greedy algorithm, which incrementally builds the EFP set. This is still computationally expensive, but (borderline) tractable.

We again start from the jet $p_T$ and $M_{jet}$ information, but immediately train a joint classifier using each of the EFPs as an input:

$$\text{NN}[p_T, M_{jet}, \text{EFP}].$$

We then select the EFP that yields the largest ADO with the CNN, evaluated on the full training set. In the first iteration, we select the EFP via:

$$\text{EFP}_1 = \arg\max_{\text{EFP}_n \in S} \text{ADO}\left[\text{CNN}, \text{NN}[p_T, M_{jet}, \text{EFP}]\right]_{X_{all}}.$$  \hspace{1cm} (32)

We repeat this procedure in each subsequent iteration, choosing the EFP that yields the largest improvement in ADO when combined with the previous observables:

$$\text{EFP}_n = \arg\max_{\text{EFP}_n \in S} \text{ADO}\left[\text{CNN}, \text{NN}[\ldots, \text{EFP}_{n-1}, \text{EFP}]\right]_{X_{all}}.$$  \hspace{1cm} (34)

The key difference from the black-box guided strategy is that the joint classifier is trained before evaluating the ADO, and the ADO is evaluated on the full training set, instead of the just the differently-ordered subset.

The primary computational cost of the brute force approach comes from training the joint classifier appearing in Eq. (34), which combines each EFP with the current set of observables. This has to be done for each EFP under consideration, and it is too computationally expensive to examine all 7,545 EFP graphs over multiple iterations. Therefore, we only consider a subset of graphs at each iteration, which means there is no guarantee the brute force method will perform better than the black-box guided strategy. For our purposes, our subset consists of the 54 connected graphs of degree $d \leq 5$ and $(\kappa, \beta)$ choices of $\kappa = [\frac{1}{2}, 1, 2] \text{ and } \beta = [\frac{1}{2}, 1, 2]$. This reduces our original search space down to a more manageable 486 choices.

The results from this brute force procedure are shown in Fig. 5 in terms of the ADO and AUC values after each iteration. In the first few iterations, the AUC and ADO values are higher than for black-box guiding, achieving a comparable performance to the original 6HL result after the inclusion of a third EFP. The brute force process continues until it matches the CNN performance with 6 EFPs (8 HL inputs total). As one would expect, the brute force approach performs well as it is effectively trying every possible combination of inputs and selecting the best. This computational cost, however, must be weighed against the marginal decrease in the number of EFPs required to match the CNN as well as the need to restrict the input space prior to exploring the performance. As

| Iteration (n) | EFP | $\kappa$ | $\beta$ | Chrom # | ADO[EFPP, CNN]$_{X_{all}}$ | AUC[EFPP] | ADO[HLN$_n$, CNN]$_{X_{all}}$ | AUC[HLN$_n$] |
|--------------|-----|---------|--------|--------|-----------------|-----------|-----------------|-----------|
| 0            | $M_{jet}$ + $p_T$ | -      | -      | -      | 0.9259          | 0.9119    |                 |           |
| 1            | $\cdot$ | 2      | $\frac{1}{2}$ | 2      | 0.8144          | 0.8190    | 0.9570          | 0.9382    |
| 2            | $\cdot$ | 0      | 2      | 2      | 0.6377          | 0.8106    | 0.9673          | 0.9458    |
| 3            | $\cdot$ | 0      | -      | 1      | 0.5460          | 0.6737    | 0.9692          | 0.9476    |
| 4            | $\cdot$ | 1      | $\frac{1}{2}$ | 2      | 0.5274          | 0.8464    | 0.9712          | 0.9487    |
| 5            | $\cdot$ | -1     | -      | 1      | 0.5450          | 0.5882    | 0.9714          | 0.9504    |
| 6            | $\cdot$ | 1      | $\frac{1}{2}$ | 4      | 0.5382          | 0.7678    | 0.9734          | 0.9523    |
| 7            | $\cdot$ | -1     | $\frac{1}{2}$ | 2      | 0.5561          | 0.5957    | 0.9741          | 0.9528    |

TABLE III. The EFPs selected during each iteration of the black-box guiding strategy beginning from HLN$_0$, which uses just $p_T$ and $M_{jet}$. For each iteration, the selected EFP is the one with the largest ADO with the CNN in the differently-ordered subspace $X_{n-1}$. The physics interpretation of these various EFPs will be presented in Sec. V D.
shown in Fig. 5, the brute force approach does not complete even a single iteration before the guided approaches have converged to a complete solution.

C. Comparison to Truth-Label Guiding

In the black-box guided strategy, the CNN and the ADO similarity metric are auxiliary tools to help identify a set of EFPs that maximizes the classification performance. Assuming the EFP space is sufficiently complete and labeled samples exist, one could dispense with the CNN entirely and simply search the space of EFPs for the most powerful set that maximizes AUC, in an approach similar to that of Ref. [106]. As a computation- tionally tractable alternative to the brute force search, we test what happens when the selection of the EFP is guided by the truth labels, instead of by the ADO.

Analogously to decision ordering in Eq. (2), we define truth ordering (TO) for a pair of signal/background points \( x \) and \( x' \) and a decision function \( f \):

\[
\text{TO}[f](x, x') = \Theta(f(x) - f(x'))
\]

where 1 corresponds to \( f \) correctly ordering the points and 0 corresponds to inverted ordering. Starting again from the jet \( p_T \) and \( M_{\text{jet}} \) information, we identify the subset of event pairs that are incorrectly ordered:

\[
Y_0 = \left\{(x, x') \mid \text{TO}[\text{HLN}_0](x, x') = 0\right\}
\]

(36)

In each iteration, we find the EFP that has the highest AUC in the incorrectly-ordered subspace,

\[
\text{EFP}_n = \arg\max_{\text{EFP} \in \mathcal{S}} \text{AUC}[\text{EFP} | Y_{n-1}]
\]

(37)

construct a new joint classifier \( \text{HLN}_n \equiv \text{HLN}_0 + n \text{EFP} \), and identify the next incorrectly-ordered subset of events:

\[
Y_n = \left\{(x, x') \mid \text{TO}[\text{HLN}_n](x, x') = 0\right\}
\]

(38)

Note that this procedure is completely independent of the CNN.

The results from this truth-label guided procedure are shown in Fig. 5 in terms of the AUC and ADO. In the first iteration, the classification performance is better than in the black-box guided search, which makes sense since the label guided method is trying to optimize AUC directly. After 7 iterations, though, the classification performance never rises above AUC = 0.951. As mentioned in Sec. 11B isolating the incorrectly-ordered pairs turns out to be counter productive, since some of these pairs could never be ordered correctly even by the optimal classifier. This emphasizes the value of using the ADO relative to an already-trained network, to make sure attention is focused on event pairs that have a chance to be correctly ordered.

D. Physics Interpretation

By translating the CNN into a space of physically-motivated observables, we can gain physical insight into the observables used in the classification decision. In particular, the first few observables in Table III give us a glimpse at a possible alternative history for the field of jet substructure, if combinations like \( C_2 \) and \( D_2 \) had not been previously identified. Distributions of the EFPs found in the first four iterations are shown in Fig. 7.

After \( p_T \) and \( M_{\text{jet}} \), the first EFP selected by the black-
The fact that a $\kappa = 2$ observable shows up early in the iterative procedure bolsters the evidence from Sec. IV A that these kinds of observables are important for mapping the CNN strategy. This is a chromatic number $c = 2$ graph, so just like jet mass, it probes deviations from 1-prong substructure. However, it uses a 5-point correlator (unlike mass which is a 2-point correlator) and it uses the $\beta = \frac{1}{2}$ angular exponent (unlike mass which uses $\beta = 2$). Putting these together, Eq. (39) is an IRC-unsafe probe of hard, small-angle radiation.

The second EFP is also IRC unsafe and also corresponds to a $c = 2$ graph:

$$\kappa = 0, \beta = 2.$$(40)

Here, though, we have $\kappa = 0$ and $\beta = 2$, which is a probe of soft, wide-angle radiation. It is interesting that the black-box guided strategy selects these two complementary $c = 2$ observable in the first two iterations, indicating the importance of 1-prong substructure probes even if the goal is to identify 2-prong boosted $W$ bosons.

The third EFP is constituent multiplicity, as seen before in Eq. (25), which reinforces the idea that controlling the composition of the quark/gluon background is important for $W$ tagging. These three observables, together with $p_T$ and $M_{jet}$, yield an AUC of 0.9476. This is not as good as the 6HL combination, but still quite encouraging given that we did not give the black-box guided strategy any information about the ratio structures used to construct $C_2$ and $D_2$.

The main surprise from this study is that IRC-safe information was not selected by the black-box guided search until the fourth iteration:

$$\kappa = 1, \beta = \frac{1}{2}.$$(41)

Moreover, it is a $c = 2$ graph, so still a probe of 1-prong substructure. Only in interaction six do we finally see a higher chromatic number graph, but the guided search skips over the $C_2/D_2$-like graphs with $c = 3$ and goes straight to $c = 4$. The black-box guided strategy has identified a very different strategy for boosted $W$ boson tagging that nevertheless matches the 6HL combination with a comparable number of observables.

One interpretation of this result is that it simply reflects the “entropy” of our HL space. There are 4 times as many IRC-unsafe observables in our HL collection than IRC-safe ones, so just by random chance, one expects to see more unsafe observables in the scan. Indeed, there are IRC-safe observables that are highly ranked in the first three iterations, just not at the top of the list. Another interpretation is that the black-box guided strategy is teaching us that IRC-unsafe information is more relevant for boosted $W$ tagging than one might naively think. A related observation was made in Ref. [83], which introduced a color ring observable to identify color-singlet configurations. Intriguingly, when restricted to three particles, the angular structure of Eq. (39) defines similar decision boundaries to the color ring. Either way, by searching through a large space of HL observables in a systematic way, the black-box guided strategy has given us a new perspective on an old problem in a human-readable format.

VI. DISCUSSION

The ever increasing complexity of new ML strategies has produced better classification performance for various physics problems. At the same time, the increasing opaqueness of these methods has widened the gap between our understanding of a problem and our appreciation of the ML solution. In this paper, we have proposed a new technique for mapping an ML solution into a space of human-interpretable observables. Our guided strategies mitigate some of the well-founded concerns about black-box approaches, while still allowing us to capitalize on the black-box performance to efficiently guide the selections of HL observables. The end result is a set of HL observables that have a more direct physical interpretation and allow for a more transparent treatment of systematic uncertainties.

In our jet substructure case study, we have shown that the black-box guided strategy could be used to isolate information that is not captured by previous HL representations. Remarkably, only a single observable was needed to close the performance gap identified in Ref. [29], nearly duplicating the CNN strategy with a low-dimensional input representation. Beginning from a minimal set of basic jet observables ($p_T$ and $M_{jet}$), we successfully condensed the CNN behavior to a small set of EFP observables which reproduce its performance and very nearly match its decisions.

Interestingly, the structure of the selected EFPs differ in qualitative ways from the $C_2$ and $D_2$ jet substructure observables custom designed for boosted $W$ boson classification. While these previous observables are based on fully connected graphs, the guided strategy picked out multi-node EFP graphs with relatively low chromatic number. While these previous observables use the IRC-safe choice of $\kappa = 1$, the guided strategy emphasized the importance of unsafe $\kappa = 2$ observables, particularly ones with non-trivial angular dependence. This motivates further physics studies of these exotic EFPs. It is worth emphasizing that we were only able to identify these new observables because we considered a sufficiently large space

4 We thank Andrew Larkoski for discussions of this point.
of HL observables. There may be other hidden organizing principles to exploit for jet substructure studies, which motivates the construction of alternative sets of observables based on different physical principles than the EFPs. In particular, we did not capitalize on the power counting and scaling properties of ratio/product observables \cite{62, 102, 106–108}, which may reveal more efficient HL observables for jet classification. It may also be beneficial to leverage first-principles knowledge about signal/background likelihood ratios \cite{83, 109–114} to identify promising HL observables.

These results have important implications for what we should regard as “best practices” in the application of ML methods to high-energy physics problems. Primarily, we should be more wary of utilizing opaque ML strategies which obscure how a problem is solved in exchange for relatively small classification improvements. In general, one should evaluate whether “additional” information captured by DNNs represents genuine patterns or is the byproduct of something unintentionally pressed into the data during simulation and then re-discovered by the network.

The informational gap in our benchmark problem could be closed using a single HL observable, suggesting that the CNN strategy was not relying on subtle correlations among the low-level features, but rather exploiting information encodable into a $\kappa = 2$ EFP. Thus, instead of a purely performance-oriented approach, we suggest a strategy of using deep networks to establish performance benchmarks, but always seek to translate ML strategies into a more tractable space of well-motivated physical observables. If this proves to be impossible or impractical, it might be that the ML approach really is identifying genuinely new information, or more likely, that the space of physical observables needs to be augmented or optimized.

More broadly, our view is that the ultimate goal of ML research in high-energy physics should not be to develop artificial-intelligence physicists which (or should we say who?) can blindly process raw data and make statements about the Universe without being able to communicate the intermediate steps. The power of modern ML can certainly be used to identify gaps in our knowledge where existing human-engineered approaches are insufficient. At the end of the day, though, we should insist that data analysis strategies used to make statements about physics should be understandable to human physicists.

**ACKNOWLEDGMENTS**

We thank Pierre Baldi, Timothy Cohen, Michael Fen-ton, Patrick Komiske, Andrew Larkoski, Eric Metodiev, Benjamin Nachman, Peter Sadowski, and Edison Weik for helpful conversations and feedback. JT was supported by the U.S. Department of Energy (DOE), Office of Science under Grant No. DE-SC0009920. TF was supported by the National Science Foundation under Award No. 1633631.

**Appendix A: Network Architectures and Hyperparameters**

For consistency, all neural networks, regardless of input data type, use a set of common settings and training procedures:

- $N = 5 \times 10^6$ training samples, broken down as:
  - 70% training,
  - 15% validation,
  - 15% testing.
- Training samples are pre-processed via sci-kit’s `StandardScaler`.
- Adam optimizer used with default `tensorflow` settings:
  - learning_rate = 0.001,
  - beta1 = 0.9,
  - beta2 = 0.999,
  - epsilon = 1e-07,
  - amsgrad = False.
- Output layer uses a `sigmoid` activation.
- Uncertainties are calculated via a 10-fold cross-validation (see App. A3).
- Early stopping on `validation_loss` with a patience of 30 epochs.
- Model checkpoints saved (for best results only) on minimum validation loss.

1. **Baseline Convolutional Neural Network**

The following training details are specific to all convolutional neural networks trained on jet-images:

- Input data undergoes a log transformation prior to `StandardScaler` pre-processing.
- Hidden layers consist of 5 hidden convolutional layers with the parameters:
  - 500 nodes,
  - kernel_size = (4,4),
  - strides = (1,1),
  - padding = 'valid',
  - kernel_initializer = 'glorot_normal',
  - activation = 'relu',
  - kernel_constraint = max_norm(3).
- 3 dropout layers (i.e. 1 between each convolutional layer) with a rate of 0.2.
2. Baseline Dense Neural Network

The following training details are specific to all dense neural networks acting on jet substructure observables, including EFPs:

- Hidden layers consist of 3 hidden dense layers with the parameters:
  - 300 nodes,
  - activation = 'relu',
  - kernel_constraint = max_norm(3).

- 2 dropout layers (i.e. 1 between each dense layer) with a rate of 0.5.

3. K-fold Validation

To derive uncertainties on the trained model prediction accuracy, we use the bootstrap cross-validation package in scikit-learn to equally divide the test set 10 times and measure the performance across 10 bootstrapping iterations. Averages and standard deviations are then taken from these 10 iterations to define the central value and uncertainties of the AUC.
Patrick T. Komiske, Eric M. Metodiev, and Matthew D. Schwartz, “Deep learning in color: towards automated quark/gluon jet discrimination,” JHEP 01, 110 (2017) [arXiv:1612.01551 [hep-ph]]

Anders Andreassen, Patrick T. Komiske, Eric M. Metodiev, Benjamin Nachman, and Jesse Thaler, “OmniFold: A Method to Simultaneously Unfold All Observables,” Phys. Rev. Lett. 124, 182001 (2020) [arXiv:1911.09107 [hep-ph]]

Kastuv Datta, Deepak Kar, and Debarati Roy, “Unfolding with Generative Adversarial Networks,” (2018), arXiv:1806.00435 [physics.data-an]

Marco Beilgente, Anja Butter, Gregor Kasieczka, Tilman Plehn, Armand Rousselot, Ramon Winterhalder, Lynton Ardizzone, and Ulrich Köthe, “Invertible Networks or Partons to Detector and Back Again,” (2020) [arXiv:2006.06685 [hep-ph]]

Christoph Englert, Peter Gallen, Philip Harris, and Michael Spannowsky, “Machine Learning Uncertainties with Adversarial Neural Networks,” Eur. Phys. J. C 79, 4 (2019) [arXiv:1807.08763 [hep-ph]]

James Barnard, Edmund Noel Dawe, Matthew J. Dolan, and Nina Rajcic, “Parton Shower Uncertainties in Jet Substructure Analyses with Deep Neural Networks,” Phys. Rev. D 95, 014018 (2017) [arXiv:1609.00607 [hep-ph]]

Benjamin Nachman, “A guide for deploying Deep Learning in LHC searches: How to achieve optimality and account for uncertainty,” SciPost Phys. 8, 090 (2020) [arXiv:1909.03081 [hep-ph]]

Patrick T. Komiske, Eric M. Metodiev, and Jesse Thaler, “Energy flow polynomials: A complete linear basis for jet substructure,” JHEP 04, 013 (2018) [arXiv:1712.07124 [hep-ph]]

Eric M. Metodiev, Benjamin Nachman, and Jesse Thaler, “Classification without labels: Learning from mixed samples in high energy physics,” JHEP 10, 174 (2017) [arXiv:1708.02949 [hep-ph]]

Anders Andreassen, Ilya Feige, Christopher Frye, and Matthew D. Schwartz, “JUNIPR: a framework for Unsupervised Machine Learning in Particle Physics,” Eur. Phys. J. C 79, 102 (2019) [arXiv:1804.09720 [hep-ph]]

Jack H. Collins, Kiel Howe, and Benjamin Nachman, “Anomaly Detection for Resonant New Physics with Machine Learning,” Phys. Rev. Lett. 121, 241803 (2018) [arXiv:1805.02664 [hep-ph]]

Cristian Buciuundefined, Rich Caruana, and Alexandru Niculescu-Mizil, “Model compression,” in Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining KDD ’06 (Association for Computing Machinery, New York, NY, USA, 2006) p. 535–541.

Javier Duarte et al., “Fast inference of deep neural networks in FPGAs for particle physics,” JINST 13, P07027 (2018) [arXiv:1804.06013 [physics.ins-det]]

Spencer Chang, Timothy Cohen, and Bryan Ostdiek, “What is the Machine Learning?” Phys. Rev. D 97, 056009 (2018) [arXiv:1709.10106 [hep-ph]]

A. A. Alemi, I. Fischer, J. V. Dillon, and K. Murphy, “Deep Variational Information Bottleneck,” ArXiv e-prints (2016) [arXiv:1612.00410 [cs.LG]]

Stefan Wunsch, Raphael Friese, Roger Wolf, and Günter Quast, “Identifying the relevant dependencies of the neural network response on characteristics of the input space,” Comput. Softw. Big Sci. 2, 5 (2018) [arXiv:1803.08782 [physics.data-an]]

Thomas Röxlo and Matthew Reece, “Opening the black box of neural nets: case studies in stop/top discrimination,” (2018) [arXiv:1804.09278 [hep-ph]]

M. G. KENDALL, “A new measure of rank correlation,” Biometrika 30, 81–93 (1938)

M.H. Seymour, “Tagging a heavy Higgs boson,” in ECFA Large Hadron Collider (LHC) Workshop: Physics and Instrumentation (1991) pp. 557–569.

Michael H. Seymour, “Searches for new particles using cone and cluster jet algorithms: A Comparative study,” Z. Phys. C 62, 127–138 (1994)

J.M. Butterworth, B.E. Cox, and Jeffrey R. Forshaw, “WW scattering at the CERN LHC,” Phys. Rev. D 65, 096014 (2002) [arXiv:hep-ph/0201098]

J.M. Butterworth, John R. Ellis, and A.R. Raklev, “Reconstructing sparticle mass spectra using hadronic decays,” JHEP 05, 033 (2007) [arXiv:hep-ph/0702150]

Jonathan M. Butterworth, Adam R. Davison, Mathieu Rubin, and Gavin P. Salam, “Jet substructure as a new Higgs search channel at the LHC,” Phys. Rev. Lett. 100, 242001 (2008) [arXiv:0802.2470 [hep-ph]]

A. Abdesselam et al., “Boosted objects: A Probe of beyond the Standard Model physics,” Boost 2010 Oxford, United Kingdom, June 22–25, 2010, Eur. Phys. J. C71, 1661 (2011) [arXiv:1012.5412 [hep-ph]]

A. Altheimer et al., “Jet Substructure at the Tevatron and LHC: New results, new tools, new benchmarks,” BOOST 2011 Princeton, NJ, USA, 22–26 May 2011, J. Phys. G39, 063001 (2012) [arXiv:1201.0008 [hep-ph]]

Jesse Shelton, “Jet Substructure,” in Theoretical Advanced Study Institute in Elementary Particle Physics: Searching for New Physics at Small and Large Scales (2013) pp. 303–340, arXiv:1302.0260 [hep-ph]

A. Altheimer et al., “Boosted objects and jet substructure at the LHC. Report of BOOST2012, held at IFIC Valencia, 23rd-27th of July 2012,” BOOST 2012 Valencia, Spain, July 23–27, 2012, Eur. Phys. J. C74, 2792 (2014) [arXiv:1311.2708 [hep-ex]]

D. Adams et al., “Towards an Understanding of the Correlations in Jet Substructure,” Eur. Phys. J. C 75, 409 (2015) [arXiv:1504.00679 [hep-ph]]

Roman Kogler et al., “Jet Substructure at the Large Hadron Collider: Experimental Review,” Rev. Mod. Phys. 91, 045003 (2019) [arXiv:1803.06991 [hep-ex]]

Simone Marzani, Gregory Soyez, and Michael Spannowsky, “Looking inside jets: an introduction to jet substructure and boosted-object phenomenology,” Vol. 958 (Springer, 2019) [arXiv:1901.10342 [hep-ph]]

Yanou Cui, Zhenyu Han, and Matthew D. Schwartz, “W-jet Tagging: Optimizing the Identification of Boosted Hadronically-Decaying W Bosons,” Phys. Rev. D 83, 074023 (2011) [arXiv:1012.2077 [hep-ph]]
