

Enforcing Interpretability and its Statistical Impacts: Trade-offs between Accuracy and Interpretability

GINTARE KAROLINA DZIUGAITE, Element AI

SHAI BEN-DAVID, University of Waterloo, Vector Institute

DANIEL M. ROY, University of Toronto, Vector Institute

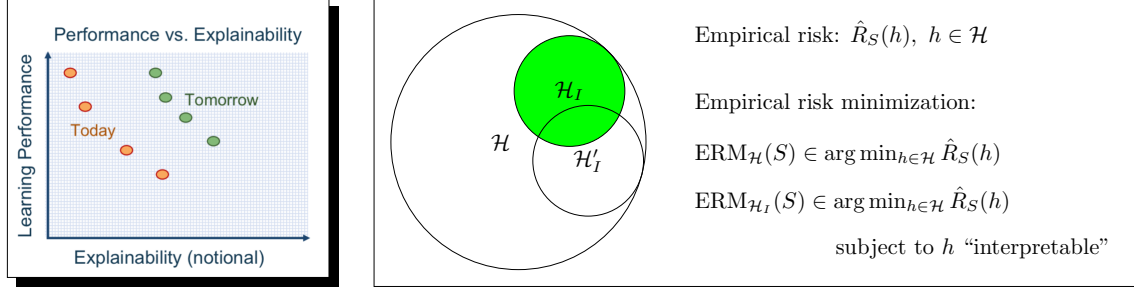


Fig. 1. (left) Figure from DARPA XAI presentation, suggesting inherent tradeoff between explainability and performance. (right) In this work, we model the act of enforcing interpretability as a constraint on learning. We adopt empirical risk minimization as a concrete model for the learning algorithm.

To date, there has been no formal study of the statistical cost of interpretability in machine learning. As such, the discourse around potential trade-offs is often informal and misconceptions abound. In this work, we aim to initiate a formal study of these trade-offs. A seemingly insurmountable roadblock is the lack of any agreed upon definition of interpretability. Instead, we propose a shift in perspective. Rather than attempt to define interpretability, we propose to model the *act of enforcing* interpretability. As a starting point, we focus on the setting of empirical risk minimization for binary classification, and view interpretability as a constraint placed on learning. That is, we assume we are given a subset of hypothesis that are deemed to be interpretable, possibly depending on the data distribution and other aspects of the context. We then model the act of enforcing interpretability as that of performing empirical risk minimization over the set of interpretable hypotheses. This model allows us to reason about the statistical implications of enforcing interpretability, using known results in statistical learning theory. Focusing on accuracy, we perform a case analysis, explaining why one may or may not observe a trade-off between accuracy and interpretability when the restriction to interpretable classifiers does or does not come at the cost of some excess statistical risk. We close with some worked examples and some open problems, which we hope will spur further theoretical development around the tradeoffs involved in interpretability.

1 INTRODUCTION

Recent years have witnessed a blowup in the scope of applications of machine learning. ⁽¹⁾ ML-based systems now play a major role in data analysis, prediction/forecasting, and decision-making support. Among the tasks that machine learning is applied to, many have significant impact on people, especially those involving medical, judicial, and financial

⁽¹⁾ DR: You can add comments like this, Shai.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2020 Copyright held by the owner/author(s).

decisions. It is no surprise that, when ML-based algorithms take part in such critical decisions, there is a demand to understand the way decisions are made—in other words, there is a demand for interpretability.

A naturally arising question is whether there are some inherent trade-offs between the “interpretability” of an algorithm and its potential power (be it the scope of situations it can handle, the accuracy of its output or any other measure of performance). This question is especially pertinent in light of the success of “black box” deep learning, one of the driving forces behind the adoption of ML.

Although there is no accepted definition of interpretability, one still finds strong assertions about its relationship with accuracy in the literature. In particular, the idea that, as one demands more interpretability, one suffers in accuracy is engrained in the literature on interpretability [3, 4, 13, 20, 23]. At the same time, there is a growing body of work suggesting that there is evidence that interpretability does not come at some inherent cost [9, 15, 16].

Is there only one possible relationship between interpretability and accuracy? What are the mechanisms underlying the relationship between interpretability and accuracy? Given how important both interpretability and accuracy are to the widespread adoption and success of machine learning and AI, it is critical that we approach this question formally.

In this work, we aim to clarify the possible statistical costs of learning interpretable classifiers. The task of formalizing interpretability, however, faces numerous obstacles.

One of the key obstacles is the lack of agreement as to the meaning of interpretability. There is a great diversity of approaches to interpretability. Despite this, we would like to develop theory that is relevant to as broad a swath of work as possible. One option would be to adopt a popular perspective on interpretability. For example, much work holds up sparse linear predictors as exemplars of interpretability. Interpretability is, however, not an inherent property of a classifier, as it depends on numerous factors, including the context, task, and audience [6].

Rather than attempting to *define* or *quantify* interpretability, we instead focus on the *act* of *enforcing* interpretability during learning. We begin with the framework of empirical risk minimization, a simple but powerful approach to learning that is well understood theoretically. We then view interpretability as placing a *constraint* on learning. In particular, if \mathcal{H} denotes the hypothesis set over which we are performing (unconstrained) empirical risk minimization, we view interpretability as constrained empirical risk minimization over some set $\mathcal{H}_I \subseteq \mathcal{H}$ of “interpretable” classifiers.

Rather than working with a particular constraint, associated to a particular notion of interpretability, we develop a theory that is as agnostic as possible to the constraint. That is, we aim to draw useful conclusions that depend as little as possible on specific details of \mathcal{H}_I . Indeed, some conclusions that we highlight depend only on the fact that \mathcal{H}_I is a subset of \mathcal{H} . It is easy to be confused by the level of generality of our arguments. Conclusions that hold for arbitrary subsets are consequences of constrained learning and not any specific detail of a notion of interpretability. It is a mistake, however, to assume that we do not learn anything about interpretability. When interpretability functions as a constraint—as it is modeled here—consequences of constrained learning are also those of enforcing interpretability.

The set $\mathcal{H}_I \subseteq \mathcal{H}$ of interpretable classifiers is presumed to be possibly dependent on the task at hand, the audience interpreting the classifiers, etc. We will, however, assume that the determination of whether a classifier is interpretable or not is independent of the training data, S . We briefly discuss how this assumption can be relaxed. Note that we do not preclude the use of heldout data in the determination of interpretability. Indeed, any presumed data-distribution dependence would likely be achieved statistically, using held out data.

Finally, we also touch upon the computational aspects of empirical risk minimization. It is well known that constrained optimization can be more costly than unconstrained minimization. Viewed from the perspective of interpretability as a constraint, this implies that insisting on interpretability can come at a computational cost as well. We give a concrete

example of this, where learning a simple logical formula explaining the data is intractable, while learning a larger, ostensibly less interpretable formula is tractable.

The model we propose here is admittedly simplified, yet we hope that it inspires more sophisticated models and more generally draws attention to the need to build formal models of interpretability and the inherent tradeoffs it brings.

1.1 Contributions

- (1) We propose to study the *act of enforcing* interpretability as a constraint on learning, allowing us to work orthogonally to those seeking to define interpretability itself.
- (2) We seek out conclusions that are agnostic to the particular notion of interpretability being enforced, allowing us to derive conclusions that are widely applicable.
- (3) We provide a summary of key results from statistical learning theory on the framework of empirical risk minimization, linking these to consideration of constrained empirical risk minimization.
- (4) We provide a case analysis of trade-offs between accuracy and interpretability, showing how each possible relationship can arise.
- (5) We describe how computational complexity can increase when seeking interpretability through constraints, highlighting another trade-off.

2 RELATED WORK

Doshi-Velez and Kim [6] discuss important aspects that need to be considered for quantifying interpretability. The meaning of a useful or informative interpretation varies with the audience consuming the interpretations, and with the purpose of having the interpretations in the first place. The theory developed in this work is valid under any criteria meeting reasonable conditions of interpretability. We discuss this further in Section 3.

Caruana et al. [3], Choi et al. [4] discuss the importance of having interpretable models in healthcare. The authors highlight that uninterpretable models are rejected despite them outperforming interpretable ones, and reiterate that “a tradeoff must be made between accuracy and intelligibility” [3]. Such statements can be found in multiple other articles outside the healthcare regime (see, e.g., [8, 10, 22, 23], among many others).

On the other hand, a number of articles report the existence of models that have no accuracy versus interpretability trade-off. Rudin [16] gives examples of interpretable yet accurate state-of-the-art models, questioning the trade-off and the need for black-box models. The author also gives examples for which choosing interpretable classifiers led to a significant increase in performance. As another example consider the algorithm proposed in [9], which learns interpretable classifiers that perform just as well as uninterpretable ones on a number of classification tasks in healthcare. Ribeiro et al. [15] propose a method for explaining classifier’s predictions. They find that more interpretable models generalize better.

The most relevant work is by Semenova and Rudin [17], where the authors propose a theoretical tool to identify the existence of simpler-yet-accurate models for a given problem. This work can be viewed as providing evidence that refutes the interpretability-versus-performance trade-off. In our case analysis, this setting is captured by the case when the excess approximation error associated to the subclass of interpretable classifiers is small compared to the gains in estimation error.

In Section 4, we discuss how the phenomena discussed in those papers, observed tradeoffs in some cases and performance gains of interpretable models in others, is not contradictory and can be clearly understood via the basic principles of our analysis.

3 FORMAL MODEL

We now introduce the formal learning model that we use to study the interpretability–accuracy tradeoff. In particular, we study supervised classification using tools from statistical learning theory. For a thorough introduction to the concepts discussed here, we refer the readers to the book by Shalev-Shwartz and Ben-David [18].

In supervised classification, we are given training examples in the form of pairs (x, y) where x is an *input* and y is a *label*. Let \mathcal{X} denote a set of possible inputs and let \mathcal{Y} denote a finite set of possible labels. Let $\mathcal{X} \rightarrow \mathcal{Y}$ denote the set of all classifiers, i.e., functions from \mathcal{X} to \mathcal{Y} .

For example, in a medical image diagnosis problem, \mathcal{X} could be the set of all bitmap images of a certain dimension, and \mathcal{Y} might be the two-point set $\{\pm 1\}$, with 1 indicating disease is present and -1 indicating no disease is present.

On the basis of training examples, we wish to learn a classifier $f \in \mathcal{X} \rightarrow \mathcal{Y}$ that will work well on new inputs that we may face in the future. There are several ways to formalize this. In statistical learning theory, we assume the training examples are randomly chosen. In particular, we assume they are independent and identically distributed from some unknown distribution \mathcal{D} on labelled inputs, $\mathcal{X} \times \mathcal{Y}$. We may then define the probability of misclassification, or *risk*,

$$R_{\mathcal{D}}(h) = \mathbb{P}_{(x,y) \sim \mathcal{D}}[h(x) \neq y]. \quad (1)$$

While \mathcal{D} is presumed to be unknown, we possess m independent and identically distributed training examples, $S \sim \mathcal{D}^m$. Writing $S = ((x_1, y_1), \dots, (x_m, y_m))$, we may define the *empirical risk* of any classifier $h \in \mathcal{H}$ by

$$\hat{R}_S(h) = \frac{\#\{0 \leq i \leq m : h(x_i) \neq y_i\}}{m}. \quad (2)$$

Writing \mathbb{E} for expectation over samples of a fixed size generated i.i.d. by the distribution \mathcal{D} , it is easy to see that, for every sample size m and every fixed classifier h (i.e., independent from S), $R_{\mathcal{D}}(h) = \mathbb{E}_{S \sim \mathcal{D}^m} \hat{R}_S(h)$. Note that this identity does not, in general, hold if h depends on S .

3.1 Interpretability as a Constraint

In order to study the trade-off between interpretability and accuracy, we must formalize interpretability in some way. There is, however, no agreed upon definition of interpretability. Arguably, interpretability can mean very different things in different situations. This is true even in the context of supervised classification.

As a starting point, we note that every learning setup implicitly works within some strict subset of the space $\mathcal{X} \rightarrow \mathcal{Y}$ of all classifiers. We will let \mathcal{H} denote the space of hypotheses under consideration. It is important to note that \mathcal{H} will not be assumed to be a subset of $\mathcal{X} \rightarrow \mathcal{Y}$. One should think of \mathcal{H} as a space of *representations* of classifiers. For example, \mathcal{H} may be the set of all neural network classifiers of some fixed depth and width, represented, e.g. by matrices of real-valued weights. This space is not a function space because two distinct set of weights may represent the same classifier on \mathcal{X} . We make this distinction because we will allow for the possibility that one representation of a classifier may be deemed interpretable while another representation may not.

Rather than attempt to define interpretability, we consider instead the effect of *demanding* interpretability, i.e., we model interpretability as a constraint on learning. In particular, we make the simplifying assumption that, for every classifier in \mathcal{H} , there is a judgment whether the classifier is *interpretable* or *not*. This approach sidesteps the question of how to define interpretability and commits only to the idea that this judgment can be made for each classifier. This judgment need not be universal—it can be considered to be specific to the problem at hand. However, crucially, the

judgment is not allowed to depend on the training samples, although it could depend on some held out samples or the data distribution, if known. That is, the judgment whether the classifier is interpretable can be task specific.

We briefly provide a few examples. If \mathcal{H} were a set of decision trees, we might define \mathcal{H}_I by a limitation on the size/depth of the tree. If \mathcal{H} were the set of neural networks of varying depth, then the set of linear predictors \mathcal{H}_I can be obtained as those without a hidden layer. In the context of vision and image classification, we might use tools to highlight image regions that most influence the logits of a neural network (say, as measured by certain gradients). Given a held out data set, we might define \mathcal{H}_I to be the set of classifiers h such that a (theoretical) group of human annotators think that the highlighted regions are sensible. Building a formal, analytical description of \mathcal{H}_I in this case would be challenging. Nevertheless, it is a formal subset of \mathcal{H} .

Consider another example based on a frequently encountered approach to interpretability. Under this approach, a classifier h is deemed interpretable if its predictions can be approximated with a small number of surrogate classifiers in an “interpretable” hypothesis class (such as sparse linear predictors). We can form our interpretable hypothesis space \mathcal{H}_I as the set of all classifiers $h \in \mathcal{H}$ that are well-approximated with, say, high-probability, by classifiers in this “interpretable” hypothesis class.

This perspective of interpretability-as-constrained-learning clearly does not encompass all approaches to interpretability. For example, we do not allow for the possibility that different people may make different judgments about interpretability, which might motivate one to not model interpretability in a binary way, as we have. As another example, we do not consider the idea that interpretability should be judged at the level of individual predictions. Our simplified formalization, however, allows us to make progress on the question of how working with interpretability *as a constraint* interacts with accuracy. We return to limitations of our formalization in Section 6.

Because every classifier in \mathcal{H} is either interpretable or not, we may define the subset, \mathcal{H}_I , of all interpretable classifiers in \mathcal{H} . Having formalized interpretability as identifying a subset of a larger hypothesis space, statistical learning theory immediately yields insight into the possible effects of restricting our attention to interpretable classifiers. Because these results are agnostic to the particular definition of interpretability, we gain insight into the trade-off between interpretability and accuracy for a wide range of situations.

3.2 Decomposing the error of a learned classifier

Let \mathcal{H} be the hypothesis space of classifiers, viewed as functions from a space \mathcal{X} of inputs to a space \mathcal{Y} of labels. One can think of this as some set of classifiers chosen to model some observed phenomena, or the set of all classifiers that some learning algorithm may output (as its input ranges over all possible training samples).

Let $A(S)$ denote the output of the learner on training data S . Note that, because the data S are assumed to be random, the hypothesis $A(S)$ is itself a random variable. Indeed, the same is true for its risk $R_{\mathcal{D}}(A(S))$ and its empirical risk $\hat{R}_S(A(S))$. As we care about the typical outcome of learning, we are interested in the distribution of these random variables.

Our primary focus is the risk of the learned classifier. However, to understand how interpretability relates to risk, we decompose the risk further.

More formally, let $R_{\mathcal{D}}^*(\mathcal{H}) = \min_{h \in \mathcal{H}} R_{\mathcal{D}}(h)$ be the minimum achievable risk by classifiers in \mathcal{H} .¹ For a learning algorithm A , let \mathcal{H}_A be the class of all classifiers that A may output, given access to any training sample. Then the risk

¹Formally, the minimum may not exist, even if there is a greatest lower bound (i.e., infimum), and so we should have written \inf rather than \min . However, we ignore such issues here. Similarly, we use \max in some places where we ought to use \sup to refer to a least upper bound, i.e., supremum.

of a classifier $A(S)$ can be decomposed as

$$\begin{aligned} R_{\mathcal{D}}(A(S)) &= R_{\mathcal{D}}^{\star}(\mathcal{H}_A) && \text{approximation error} \\ &+ R_{\mathcal{D}}(A(S)) - R_{\mathcal{D}}^{\star}(\mathcal{H}_A) && \text{estimation error} \end{aligned}$$

The first component, $R_{\mathcal{D}}^{\star}(\mathcal{H}_A)$, is the *approximation error* and is independent of the training sample. It is a property of the learning algorithm A (or the class models, or hypotheses, considered). It may be thought of as the *bias* implied by the choice of learning tool.

The second component, $R_{\mathcal{D}}(A(S)) - R_{\mathcal{D}}^{\star}(\mathcal{H}_A)$, is *estimation error*. Estimation error quantifies how close we are to the best hypothesis in \mathcal{H} . When h is the output $A(S)$ of a learning algorithm, estimation error arises due to overfitting. Informally, estimation error arises due to variability in the data (informally, variance).

It is important to highlight that, as a machine-learning user, we are not interested in the individual errors in risk decomposition in isolation. Our interest is in the risk of the output classifier. However, as we will explain, the interplay between the different types of errors is key to understanding the effects of an interpretability constraint on the risk.

Using the fact that the class of interpretable classifiers is a subset of a larger hypothesis class, i.e., $\mathcal{H}_I \subseteq \mathcal{H}$, we can immediately conclude that

$$R_{\mathcal{D}}^{\star}(\mathcal{H}) = \min_{h \in \mathcal{H}} R_{\mathcal{D}}(h) \leq \min_{h \in \mathcal{H}_I} R_{\mathcal{D}}(h) = R_{\mathcal{D}}^{\star}(\mathcal{H}_I). \quad (3)$$

This leads us to the first fact about the approximation error of interpretable classifiers.

Fact 1: \mathcal{H} has no larger approximation error than \mathcal{H}_I .

It follows that the difference between approximation error of \mathcal{H} and of \mathcal{H}_I quantifies the cost of restricting our attention to interpretable hypotheses, if we ignore estimation error.

The distribution of the estimation error of a learned hypothesis $A(S)$ characterizes the typical gap in risk between $A(S)$ and the best predictor in the class. We further analyze the estimation error in the Section 4.

3.3 Empirical Risk Minimization

The distribution of estimation error is determined, in part, by the learning algorithm. Therefore, in order to study the tradeoffs associated with interpretability, we must specify some model for how we intend to learn with and without interpretability as a constraint. Arguably, the simplest model to consider is *empirical risk minimization* (ERM) over \mathcal{H}_I and \mathcal{H} . An algorithm A performs empirical risk minimization over a hypothesis set \mathcal{H} when, for all possible data sets S , the learned classifier $A(S)$ achieves the minimum risk, i.e.,

$$\hat{R}_S(\text{ERM}_{\mathcal{H}}(S)) = \min_{h \in \mathcal{H}} \hat{R}_S(h). \quad (4)$$

We refer to a set of classifiers learned by a generic ERM algorithm by $\text{ERM}_{\mathcal{H}}(S)$, with h_{ERM} denoting an element of $\text{ERM}_{\mathcal{H}}(S)$. We may then formalize an interpretable learning algorithm as ERM over \mathcal{H}_I , yielding a classifier $h_{\text{ERM}}^0 \in \text{ERM}_{\mathcal{H}_I}(S)$.

The *generalization error*, $\text{Gen}_{\mathcal{D}}(h; S)$, of a hypothesis $h \in \mathcal{H}$ is the gap between the risk and empirical risk of h , i.e., the difference between the train and test errors. Formally,

$$\text{Gen}_{\mathcal{D}}(h; S) = |R_{\mathcal{D}}(h) - \hat{R}_S(h)|. \quad (5)$$

A key quantity is the *worst-case generalization error over \mathcal{H}* :

$$\max_{h \in \mathcal{H}} \text{Gen}_{\mathcal{D}}(h; S) \quad (6)$$

It is easy to demonstrate that the estimation error of h_{ERM} is bounded above by twice the worst-case generalization error. To see this, note that, because h_{ERM} achieves the minimal empirical risk, the empirical risk for every $h \in \mathcal{H}$ is no smaller. Thus, for every $h \in \mathcal{H}$, this logic justifies the inequality

$$R_{\mathcal{D}}(h_{\text{ERM}}) - R_{\mathcal{D}}(h) \quad (7)$$

$$= R_{\mathcal{D}}(h_{\text{ERM}}) - \hat{R}_S(h_{\text{ERM}}) + \hat{R}_S(h_{\text{ERM}}) - R_{\mathcal{D}}(h) \quad (8)$$

$$\leq \text{Gen}_{\mathcal{D}}(h_{\text{ERM}}; S) + \text{Gen}_{\mathcal{D}}(h; S) \quad (9)$$

Finally, we can bound the sum:

$$\text{Gen}_{\mathcal{D}}(h_{\text{ERM}}; S) + \text{Gen}_{\mathcal{D}}(h; S) \leq 2 \max_{h' \in \mathcal{H}} \text{Gen}_{\mathcal{D}}(h'; S). \quad (10)$$

Since this inequality holds for every $h \in \mathcal{H}$, it holds for the hypothesis $h^* = \arg \min R_{\mathcal{D}}(h)$ that achieves the minimum risk. Substituting in h^* , we obtain the desired bound on the estimation error:

$$R_{\mathcal{D}}(h_{\text{ERM}}) - R_{\mathcal{D}}^*(\mathcal{H}) \leq 2 \max_{h \in \mathcal{H}} \text{Gen}_{\mathcal{D}}(h; S) \quad (11)$$

Fact 2: The estimation error of $\text{ERM}_{\mathcal{H}}$ is bounded above by twice the worst-case generalization error over \mathcal{H} .

Next, we state another fact describing how the generalization error of interpretable classifiers relates to the generalization error of the ones in \mathcal{H} . Since $\mathcal{H}_I \subseteq \mathcal{H}$, the following inequality follows trivially:

$$\max_{h \in \mathcal{H}_I} \text{Gen}_{\mathcal{D}}(h; S) \leq \max_{h \in \mathcal{H}} \text{Gen}_{\mathcal{D}}(h; S). \quad (12)$$

Therefore, with probability one, the following fact holds:

Fact 3: The worst-case generalization error over \mathcal{H}_I is no larger than the worst-case generalization error over \mathcal{H} .

It is worth noting that the generalization error of a particular classifier returned by some learning algorithm may be much better than the worst-case generalization error, even if the algorithm is an ERM. There is a rich literature on generalization error, and a wide range of tools that have been introduced to study and quantify it [1, 2, 5, 7, 11, 12, 14, 19]. For binary classification and empirical risk minimization, the worst-case generalization error is characterized by the so-called VC dimension [21], which we briefly touch on below.

3.4 Risk decomposition for approximate ERM

In the case of approximate ERM, the output of a learner is determined by three aspects of the learning process: the search space of hypothesis considered by the learning algorithm, the training data (in particular, how representative the data are of the distribution relative to the hypothesis space), and the computational resources invested.

Accordingly, the error of an output classifier can be decomposed as the sum of the smallest empirical error achievable in the hypothesis space, the *optimization error* (i.e., the gap between the empirical error achieved within the computational resource bounds and the smallest achievable), and the *generalization error* (i.e., the gap between the empirical error of

the output classifier and its true error):

$$\begin{aligned}
& R_{\mathcal{D}}(A(S)) \\
&= \min_{h \in \mathcal{H}} \hat{R}_S(h) && \text{empirical risk of ERM} \\
&\quad + \hat{R}_S(A(S)) - \min_{h \in \mathcal{H}} \hat{R}_S(h) && \text{optimization error} \\
&\quad + R_{\mathcal{D}}(A(S)) - \hat{R}_S(A(S)) && \text{generalization error}
\end{aligned}$$

We will consider this decomposition later when studying the interplay of accuracy (risk) and interpretability.

Like with approximation error, there is a trivial relationship between the ERM risk with and without an interpretability constraint:

Fact 4: The empirical risk of ERM over \mathcal{H} is no larger than that over \mathcal{H}_I .

We discuss optimization and generalization error in more detail in the Section 4.

3.5 Quantifying Expressivity via VC Dimension

The VC dimension is a measure of the expressive power or “complexity” of a space of binary classifiers. We start by introducing the notion of *shattering*.

For any subset $X \subseteq \mathcal{X}$ and let $|X|$ denote its size. Let $\mathcal{H} \circ X$ denote the set of subsets of X of the form $\{x \in X : h(x) = 1\}$ for some $h \in \mathcal{H}$. In other words, $\mathcal{H} \circ X = \{h^{-1}(1)(x) \cap X : h \in \mathcal{H}\}$ is the set of all possible 0/1 partitions that classifiers in \mathcal{H} can induce on X . It follows that $|\mathcal{H} \circ X| \leq 2^{|X|}$. We say that \mathcal{H} *shatters* a set X if $|\mathcal{H} \circ X| = 2^{|X|}$.

If all we know about a learning algorithm is that it performs ERM over \mathcal{H} , then we cannot hope to learn from any data set that \mathcal{H} shatters. In these cases, the hypothesis space is “too complex” given the number of data. This logic is formalized by so-called “No Free Lunch” theorems. Thus understanding shattering is critical to understanding the performance of ERM.

The VC dimension of a \mathcal{H} , denoted $\text{VCdim}(\mathcal{H})$, is the size of the largest shattered set. The VC dimension tells us the size of the largest training sample we might obtain perfect classification accuracy, regardless of the true labels.

Assume $\text{VCdim}(\mathcal{H}_I) = d$. Let X be a set of d instances that \mathcal{H}_I can shatter. Then since all $h \in \mathcal{H}_I$ are also in \mathcal{H} , \mathcal{H} can also shatter S , and so \mathcal{H} has a VC dimension of at least d .

Fact 5: $\text{VCdim}(\mathcal{H}_I) \leq \text{VCdim}(\mathcal{H})$.

If $\text{VCdim}(\mathcal{H}) < \infty$, worst-case generalization error over \mathcal{H} decays to zero as the number of training data grows. This is formalized in the next fact.

Fact 6: With probability at least $1 - \delta$ over a training sample S of size m , the worst-case generalization error over \mathcal{H} satisfies

$$\max_{h \in \mathcal{H}} \text{Gen}_{\mathcal{D}}(h; S) \leq O\left(\sqrt{\frac{\text{VCdim}(\mathcal{H}) + \log 1/\delta}{m}}\right). \quad (13)$$

It follows immediately from Facts 2 and 6 that the estimation error for ERM satisfies the same inequality in Eq. (13). We summarize this consequence as follows:

Fact 7: If $\text{VCdim}(\mathcal{H}) < \infty$, the risk of every empirical risk minimizer converges to the approximation error of \mathcal{H} as the number of training data grows.

4 EFFECT OF INTERPRETABILITY ON RISK

In this section, we consider the impact of restricting our attention to interpretable classifiers, using the two risk decompositions presented in Section 3. In each case, we describe how a tradeoff between accuracy and interpretability may or may not exist.

4.1 Approximation and Estimation Error

We first start by analyzing the decomposition of risk into approximation error and estimation error. By Fact 1, we know that approximation error can never decrease by restricting one's attention to interpretable classifiers. Thus the impact of moving from \mathcal{H} to \mathcal{H}_I on accuracy (risk) is determined by whether the increase in approximation error

$$R_{\mathcal{D}}^*(\mathcal{H}_I) - R_{\mathcal{D}}^*(\mathcal{H}) \quad (14)$$

is greater than, less than, or approximately equal to the change in estimation error,

$$\begin{aligned} & (R_{\mathcal{D}}(\text{ERM}_{\mathcal{H}_I}(S)) - R_{\mathcal{D}}^*(\mathcal{H}_I)) \\ & - (R_{\mathcal{D}}(\text{ERM}_{\mathcal{H}}(S)) - R_{\mathcal{D}}^*(\mathcal{H})). \end{aligned} \quad (15)$$

As a result, we can find almost any type of tradeoff between accuracy and interpretability.

The two factors determining the estimation error of ERM are the number of training data and the effective capacity of the hypothesis class, the latter being a quantity that, in general, may depend on the data distribution.

In Fact 2, we showed that the estimation error of ERM is bounded by twice the worst-case generalization error, and in Fact 6, we quoted PAC theory bounding the worst-case generalization error in terms of the ratio of the VC dimension and the number of training data, irrespective of the data distribution. Thus, if one has a number of training data far in excess of the VC dimension of \mathcal{H} , then, irrespective of the data distribution, the estimation error of $\text{ERM}_{\mathcal{H}}$ will be small. In this case, the decrease in estimation error (Eq. (15)) is small, and so we will see no appreciable tradeoff with accuracy (if the increase in approximation error (Eq. (14)) is small) or a tradeoff (otherwise).

When the number of data are not far in excess of the VC dimension of \mathcal{H} , then the data distribution comes into play. It may be the case that a class has a large (or infinite) VC dimension, yet, relative to a specific distribution, the capacity (measured, e.g., by the covering number) is small. Indeed, it suffices for the number of training data to be far in excess of this distribution-dependent capacity of \mathcal{H} for the decrease in estimation error to be negligible. If it is not, then it is possible that, by moving to \mathcal{H}_I , one could see a significant drop in estimation error. Again, \mathcal{H}_I need only have small capacity for the actual data distribution in question. If the drop in estimation error is large, this could balance or exceed the increase in approximation error, leading to no tradeoff or even a benefit moving to the interpretable class, \mathcal{H}_I . In the latter case, we would credit the improved performance on improved generalization.

4.2 Empirical risk and generalization error

We can take another view using the decomposition of the risk into the empirical risk and the generalization error. We will focus first on (exact) empirical minimization, deferring a discussion of the role of optimization error to later.

By Fact 4, we know that the empirical risk of $\text{ERM}_{\mathcal{H}_I}(S)$ is no smaller than that of $\text{ERM}_{\mathcal{H}}(S)$. Therefore, like above, the impact of moving from \mathcal{H} to \mathcal{H}_I on accuracy (risk) is determined by whether the increase in empirical risk

$$\hat{R}_S(\text{ERM}_{\mathcal{H}_I}(S)) - \hat{R}_S(\text{ERM}_{\mathcal{H}}(S)) \quad (16)$$

is greater than, less than, or approximately equal to the sum of the change in generalization error

$$\begin{aligned} & (R_{\mathcal{D}}(\text{ERM}_{\mathcal{H}_I}(S)) - \hat{R}_S(\text{ERM}_{\mathcal{H}_I}(S))) \\ & - (R_{\mathcal{D}}(\text{ERM}_{\mathcal{H}}(S)) - \hat{R}_S(\text{ERM}_{\mathcal{H}}(S))). \end{aligned} \tag{17}$$

Like with estimation error, the change in generalization error can depend on the data distribution, but this dependence vanishes if the number of samples exceeds the effective (i.e., distribution dependent) capacity of the larger class \mathcal{H} .

The generalization error is bounded by the worst-case generalization error and so the difference in generalization errors can also be bounded in terms of twice the worst-case generalization error of the larger class, \mathcal{H} . Thus, if the number of training examples is great enough, then will be no penalty in terms of generalization error in moving to the larger class, or, in other words, no advantage in terms of generalization error in moving to the interpretable class, \mathcal{H}_I . If there is some increase in approximation error, we may expect an increase in empirical risk of ERM over \mathcal{H}_I as compared with \mathcal{H} , and thus a decrease in accuracy overall.

When the number of data are moderate, however, the interpretable class may provide much smaller generalization error (or it may not, as we address below in our discussion of fast rate bounds). If the generalization error of \mathcal{H}_I is much less, this advantage may make up for the increase in empirical risk (which may be due to increased approximation error). In this case, interpretability has a regularizing effect and leads to improved accuracy.

Heretofore, we have focused on exact ERM, whereas in practice ERM over a hypothesis class can be computational intractable. Instead, one often relies upon an approximate implementation of ERM. In Section 5, we present an example where, even though the approximation error does not change when moving to the interpretable subclass, the optimization error prevents one from learning.

4.2.1 Fast-rate bounds. Up to constants, standard generalization bounds converge to zero at a so-called “slow” rate of $O(\sqrt{C/m})$, where C is the “capacity” of \mathcal{H} , which can be distribution-dependent. For almost all notions of capacity, we have $C_I \leq C$, where C_I is the capacity of \mathcal{H}_I . As such, we might naively expect there to be an advantage moving to \mathcal{H}_I when it comes to generalization error.

However, this discussion ignores the effect of the size of risk, $R_{\mathcal{D}}(\text{ERM}_{\mathcal{H}}(S))$, on the generalization error. In particular, when the risk is small, we may be able to obtain “fast rate” bound that converges to zero as $O(C/m)$. Thus, if the approximation error of \mathcal{H} is close to zero, but the approximation error of \mathcal{H}_I is nontrivial, the improvement in capacity may be swamped by the change from a fast to a slow rate of convergence.

5 EXAMPLE: MOVING TO A LARGER CLASS FOR EFFICIENT LEARNING VIA ERM

Interpretability is not just a restriction of the expressive power of hypotheses, it is also a restriction on the representation of the classifiers. The same classifier may be represented in many ways, some more obscure and others more interpretable. A representation restriction makes it computationally harder to come up with a good classifier. The following example borrowed from [18] shows that such a hardness gap may turn a computationally feasible learning task into a computationally unfeasible one.

Consider the class of 3-term disjunctive normal form formulae (3-DNF); The instance space is $\mathcal{X} = \{0, 1\}^n$ and each hypothesis is represented by the Boolean formula of the form $h(x) = A_1(x) \vee A_2(x) \vee A_3(x)$, where each $A_i(x)$ is a Boolean conjunction (and AND of Boolean variables or negations of such). The output of $h(x)$ is 1 if either $A_1(x)$ or $A_2(x)$ or $A_3(x)$ output the label 1. If all the three conjunctions output the label 0 then $h(x) = 0$.

Let H_{3DNF}^n be the class of all such 3-DNF formulae. The size of H_{3DNF}^n is at most 3^{3d} . Hence, the sample complexity of learning H_{3DNF}^n using the ERM rule is at most $3d \log(3/\delta)/\epsilon$.

While a 3-term DNF formula may be considered interpretable, from the computational perspective, finding a low-error classifier of this form is hard. In particular, Pitt et al. [1988] and Kearns et al. [1994] showed that unless $RP=NP$, there is no polynomial time algorithm that solves the 3-term DNF learning problems in which $d_n = n$ by providing an output that is a 3-term DNF formula.

In contrast, once we relax this requirement on the representation of the output hypothesis, the learning problem becomes feasible. The key observation behind such a learner is noting that since \vee distributes over \wedge , each 3-term DNF formula can be rewritten as:

$$A_1 \vee A_2 \vee A_3 = \bigwedge_{u \in A_1, v \in A_2, w \in A_3} (u \vee v \vee w) \quad (18)$$

Next, let us define: $\psi : \{0, 1\}^n \rightarrow \{0, 1\}^{(2n)^3}$ such that for each triplet of literals u, v, w there is a variable in the range of ψ indicating if $u \vee v \vee w$ is true or false. So, for each 3-DNF formula over $\{0, 1\}^n$ there is a conjunction over $\{0, 1\}^{(2n)^3}$, with the same truth table. Since we assume that the data is realizable, we can solve the ERM problem with respect to the class of conjunctions over $\{0, 1\}^{(2n)^3}$. Furthermore, the sample complexity of learning the class of conjunctions in the higher dimensional space is at most $n^3 \log(1/\delta)/\epsilon$. Thus, the overall runtime of this approach is polynomial in n .

The resulting representation of the Boolean function is arguably less interpretable (since the resulting conjunctive formula may contain many terms, and large conjunctions of such triplets variables may be hard to interpret).

In other words, the interpretability requirement, encapsulated by asking for 3-term DNF classifiers turns an otherwise feasibly learnable problem into a computationally infeasible one.

6 DISCUSSION

We have proposed to study the relationship between accuracy (risk) and interpretability using a simplified model of learning. Namely, by focusing on empirical risk minimization and by modeling interpretability as the act of restricting one’s attention to a *subset* of classifiers that are deemed interpretable by some judgement, we can make a precise analysis of the factors that contribute to accuracy (risk) and how they are affected when we shift from performing ERM on \mathcal{H} versus its interpretable subclass \mathcal{H}_I .

One open problem posed by our work is understanding the trade-off between interpretability and accuracy when the set \mathcal{H}_I of interpretability hypotheses depends on the training sample. Our analysis above relies on the independence of \mathcal{H}_I from S , and so any dependence does not permit one to make the conclusions we have made. Recently, Foster et al. [2019] have studied data-dependent hypotheses sets using a notion of uniform stability. It would be interesting to consider how some standard approaches to explainability (which might be viewed as the evidence one uses to make a judgement as to the interpretability of a classifier) might be modified to make them “stable” and potentially amenable to an analysis using this frame.

REFERENCES

- [1] Peter L Bartlett and Shahr Mendelson. 2001. Rademacher and Gaussian complexities: Risk bounds and structural results. In *International Conference on Computational Learning Theory*. Springer, 224–240.
- [2] Olivier Bousquet and André Elisseeff. 2002. Stability and generalization. *Journal of machine learning research* 2, Mar (2002), 499–526.
- [3] Rich Caruana, Yin Lou, Johannes Gehrke, Paul Koch, Marc Sturm, and Noemie Elhadad. 2015. Intelligible models for healthcare: Predicting pneumonia risk and hospital 30-day readmission. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 1721–1730.

- [4] Edward Choi, Mohammad Taha Bahadori, Jimeng Sun, Joshua Kulas, Andy Schuetz, and Walter Stewart. 2016. Retain: An interpretable predictive model for healthcare using reverse time attention mechanism. In *Advances in Neural Information Processing Systems*. 3504–3512.
- [5] Luc Devroye and Terry Wagner. 1979. Distribution-free performance bounds for potential function rules. *IEEE Transactions on Information Theory* 25, 5 (1979), 601–604.
- [6] Finale Doshi-Velez and Been Kim. 2017. Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608* (2017).
- [7] Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Aaron Leon Roth. 2015. Preserving statistical validity in adaptive data analysis. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*. ACM, 117–126.
- [8] Leilani H Gilpin, David Bau, Ben Z Yuan, Ayesha Bajwa, Michael Specter, and Lalana Kagal. 2018. Explaining explanations: An overview of interpretability of machine learning. In *2018 IEEE 5th International Conference on data science and advanced analytics (DSAA)*. IEEE, 80–89.
- [9] Jay Heo, Hae Beom Lee, Saehoon Kim, Juho Lee, Kwang Joon Kim, Eunho Yang, and Sung Ju Hwang. 2018. Uncertainty-aware attention for reliable interpretation and prediction. In *Advances in Neural Information Processing Systems*. 909–918.
- [10] Ulf Johansson, Cecilia Sönströd, Ulf Norinder, and Henrik Boström. 2011. Trade-off between accuracy and interpretability for predictive in silico modeling. *Future medicinal chemistry* 3, 6 (2011), 647–663.
- [11] Michael Kearns and Dana Ron. 1999. Algorithmic stability and sanity-check bounds for leave-one-out cross-validation. *Neural computation* 11, 6 (1999), 1427–1453.
- [12] Vladimir Koltchinskii and Dmitriy Panchenko. 2000. Rademacher processes and bounding the risk of function learning. In *High dimensional probability II*. Springer, 443–457.
- [13] Himabindu Lakkaraju, Stephen H Bach, and Jure Leskovec. 2016. Interpretable decision sets: A joint framework for description and prediction. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. ACM, 1675–1684.
- [14] David A McAllester. 1999. PAC-Bayesian model averaging. In *COLT*, Vol. 99. Citeseer, 164–170.
- [15] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. 2016. Why should i trust you?: Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. ACM, 1135–1144.
- [16] Cynthia Rudin. 2018. Please stop explaining black box models for high stakes decisions. *arXiv preprint arXiv:1811.10154* (2018).
- [17] Lesia Semenova and Cynthia Rudin. 2019. A study in Rashomon curves and volumes: A new perspective on generalization and model simplicity in machine learning. *arXiv preprint arXiv:1908.01755* (2019).
- [18] Shai Shalev-Shwartz and Shai Ben-David. 2014. *Understanding machine learning: From theory to algorithms*. Cambridge university press.
- [19] John Shawe-Taylor, Peter L Bartlett, Robert C Williamson, and Martin Anthony. 1998. Structural risk minimization over data-dependent hierarchies. *IEEE transactions on Information Theory* 44, 5 (1998), 1926–1940.
- [20] Michael Tsang, Dehua Cheng, and Yan Liu. 2017. Detecting statistical interactions from neural network weights. *arXiv preprint arXiv:1705.04977* (2017).
- [21] Vladimir N Vapnik and A Ya Chervonenkis. 2015. On the uniform convergence of relative frequencies of events to their probabilities. In *Measures of complexity*. Springer, 11–30.
- [22] Jialei Wang, Ryohei Fujimaki, and Yosuke Motohashi. 2015. Trading interpretability for accuracy: Oblique treed sparse additive models. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 1245–1254.
- [23] Tong Wang. 2019. Gaining Free or Low-Cost Interpretability with Interpretable Partial Substitute. In *International Conference on Machine Learning*. 6505–6514.