Abstract

We address the problem of training models with black-box and hard-to-optimize metrics by expressing the metric as a monotonic function of a small number of easy-to-optimize surrogates. We pose the training problem as an optimization over a relaxed surrogate space, which we solve by estimating local gradients for the metric and performing inexact convex projections. We analyze gradient estimates based on finite differences and local linear interpolations, and show convergence of our approach under smoothness assumptions with respect to the surrogates. Experimental results on classification and ranking problems verify the proposal performs on par with methods that know the mathematical formulation, and adds notable value when the form of the metric is unknown.

1. Introduction

We consider the problem of training a machine learning model when the true evaluation metric is difficult to optimize on the training set. This general problem arises with many flavors and in different scenarios. For example, we may have a black-box metric whose mathematical expression is unknown or difficult to approximate with a convex training loss. This is the case with non-decomposable evaluation metrics, such as the F-measure or ranking metrics like Precision@K, where it is not straightforward to construct a smooth objective that closely approximates the metric.

Another example is when the training labels are only a proxy for the true label. This arises in problems where one has access to cheap-to-acquire noisy labels, such as clicks, but wishes to optimize for a more expensive label, such as whether users rate a result as good. If we have access to a small auxiliary validation set with true labels, how can this information be used to influence the training loss? Similar examples also arise when the training data has noisy features and we have a small validation set with clean features, or in machine learning fairness problems where the training data contains group-dependent noise, but we may have access to a small set of auxiliary clean data.

In many of the above scenarios, one wishes to optimize a black-box metric $M$ over $d$ model parameters, but does not have access to explicit gradients for $M$, nor is it practical to obtain reliable gradient estimates when $d$ is large. We provide a general solution to this problem by choosing $K \ll d$ convex surrogate losses, and expressing $M$ as an unknown monotonic function $\psi : \mathbb{R}^K \to \mathbb{R}$ of the $K$ surrogates. We then reformulate the original problem as an optimization of $\psi$ over the $K$-dimensional surrogate space. The choice of surrogates can be as simple as the hinge losses on positive and negative samples, which should work well for metrics like the F-measure, or the surrogates can be chosen to be a family of different convex losses to handle robustness to training noise given a small set of clean validation samples.

Our strategy is to estimate gradients for the unknown function $\psi$ with respect to its $K$ inputs by measuring changes in the metric $M$ and the $K$ surrogates for different perturbations on the model, and use the estimates for $\nabla \psi$ to perform projected gradient descent over the $K$-dimensional surrogate space. We show how the projection step can be implemented inexactly but with convergence guarantees by solving a convex problem in the original $d$ parameters. We are thus able to adaptively combine the $K$ surrogates to align well with the target metric $M$.

The main contributions of this paper include:

1. A novel formulation that poses the problem of optimizing a black-box metric as a lower-dimensional problem in a surrogate space.
2. A projected gradient descent based training algorithm using finite-differences and local linear interpolations to estimate gradients.
3. Theoretical results showing convergence to a stationary point under smoothness assumptions on $\psi$.
4. Experiments showing that the proposed approach works as well as methods that take advantage of the form of the metric if known, and can give substantial gains when the metric truly is a black-box.
2. Related Work

There has been much work on directly optimizing specialized classes of evaluation metrics during training. These include approaches that relax the metric using convex surrogates (Joachims et al., 2005; Kar et al., 2014; Narasimhan et al., 2015a; Kar et al., 2016), plug-in or post-shift methods that tune a threshold on estimates of class probabilities (Ye et al., 2012; Koyejo et al., 2014; Narasimhan et al., 2014; Yan et al., 2018), reduction approaches that formulate a sequence of cost-sensitive learning tasks (Parambath et al., 2014; Narasimhan et al., 2015b; Alabi et al., 2018; Narasimhan, 2018), and approaches that use constrained optimization and game-based formulations (Eban et al., 2017; Narasimhan et al., 2019).

However, all the above approaches require the evaluation metric to be available in closed-form. Of these, the closest to ours is the approach of Narasimhan et al. (2015b), which reformulates the learning problem as an optimization problem over the space of confusion matrices. To ensure the constraint set is convex, this approach requires the use of stochastic classifiers, and the theoretical guarantees assume that the metrics are convex or pseudo-convex in the confusion matrix. In contrast, we do not require stochastic classifiers, and can handle generic metrics.

Recently, there has been some work on optimizing evaluation metrics that are only available as a black-box. Zhao et al. (2019b) approximate black-box metrics with a weighted training loss where the weighting function acts on a low-dimensional embedding of each example, and a validation set is used to estimate the parameters of the example-weighting function. A related approach by Ren et al. (2018) uses meta-gradient descent to re-weight the training examples to handle training set biases and label noise. In contrast, we model the unknown metric as a function of surrogate losses, and directly estimate the metric gradients, rather than estimating a weighting function on each example.

Huang et al. (2019) also propose jointly adaptively learning a metric with the model training. They use a parametric form for their learned metric, whereas we nonparametrically estimate the metric gradients. They use reinforcement learning to align the training objective’s optimum with that of the true metric, whereas we use gradient descent over a surrogate space. They do not provide any theoretical guarantees.

Grabocka et al. (2019) express the metric as a set function that maps each prediction to an embedding and maps the average embedding across all examples to the predicted metric. They jointly optimize the parameters for the loss and the model. This approach is similar to ours in that it expresses the metric as a function on surrogate losses, and attempts to learn that function. However, our approach is different in two key points. First, we take as given known-useful surrogate losses, whereas they learn decomposable surrogate mappings from scratch. Second, they parameterize their surrogate functions and final mapping as neural networks, whereas we nonparametrically adaptively estimate the local gradients. They provide limited theoretical guarantees.

Similar to Grabocka et al. (2019), the work of Wu et al. (2018) also learns a parameterized metric (e.g. as a neural network). An auxiliary parametric “teacher” model is used to adaptively learn the parameters for the metric that will maximize performance on a validation set. They do not provide theoretical guarantees.

3. Problem Setup and High-level Approach

Let \( X \) be some instance space and \( Y \) be the label space. Let \( f_\theta : X \rightarrow \mathbb{R} \) be a model parametrized by \( \theta \in \mathbb{R}^d \) that outputs a score \( f_\theta(x) \) for instance \( x \in X \). One can use this score to make a prediction; e.g. for binary classification problems, one predicts \( \text{sign}(f_\theta(x)) \). We measure performance w.r.t. a test distribution \( D \) over \( X \times Y \). We consider two scenarios, one where we are provided a training sample \( S \) of \( n \) examples directly drawn from \( D \), and the other where the training sample \( S \) is drawn from a noisy distribution, and we are provided a smaller clean validation set from \( D \).

The performance of \( f_\theta \) is evaluated by a metric \( M : \mathbb{R}^d \rightarrow [0, 1] \) computed on \( D \), where \( M \) may be as simple as the error rate \( M_{err}(\theta) = \mathbb{E}_{(x,y) \sim D} [y f_\theta(x) > 0] \) (or an estimate), or \( M \) may be a complex, non-decomposable metric such as Precision@K that depends on the scores and the distribution in a more intricate manner. We consider settings where the form of \( M \) is unknown, and the metric is available only as a black-box, i.e., for a given \( \theta \in \mathbb{R}^d \), we can evaluate \( M(\theta) \). The goal is to learn a good \( \theta \) by solving:

\[
\min_{\theta \in \mathbb{R}^d} M(\theta).
\]

3.1. Reformulation with Surrogates

To optimize (1), one could directly estimate gradients of \( M \) with respect to the \( d \) parameters, but \( d \) is usually too large for that to be practical. To relax (1) to a more tractable problem, we take as given \( K \) convex surrogate loss functions \( \ell_1, \ldots, \ell_K : \mathbb{R}^d \rightarrow \mathbb{R}_+ \) where \( K \ll d \), and express \( M \) as an unknown non-decreasing function of the \( K \) surrogates, with an unknown slack:

\[
M(\theta) = \psi(\ell_1(\theta), \ldots, \ell_K(\theta)) + \epsilon(\theta),
\]

where \( \psi : \mathbb{R}^K \rightarrow [0, 1] \) is monotonic but possibly non-convex, and the slack \( \epsilon : \mathbb{R}^d \rightarrow [-1, 1] \) determines how well the metric can be approximated by the \( K \) surrogates. Note that this decomposition of \( M \) is not unique. Our results hold for any such decomposition, but to enable a tighter analysis we consider a \( \psi \) for which the associated worst-case slack over all \( \theta \), i.e., \( \max_{\theta \in \mathbb{R}^d} |\epsilon(\theta)| \) is the minimum.
Here are examples of target metrics and convex surrogates.

**Example 1 (Classification Metrics).** Consider the task of minimizing the G-mean metric given by $1 - \sqrt{\text{TPR} \times \text{TNR}}$, where TPR is the true positive rate and TNR is the true negative rate. This metric promotes high accuracies on both the positive and negative class and is popular for classification tasks where there is class imbalance (Daskalaki et al., 2006). Possible surrogates for this metric include the average logistic or hinge losses on the positive and negatives examples as these serve as proxies for the TPR and TNR. It is reasonable to assume monotonic $\psi$ here, since lower surrogate values tend to produce better TPR and TNR values, and in turn lower G-means. The F-measure is another popular metric that can be written as a monotonic function of the TPR and TNR (Koyejo et al., 2014), and there again the average positive and negative losses would make good surrogates.

**Example 2 (Misaligned Training Data).** Consider minimizing a metric using a training dataset that is noisy or misaligned with the test distribution, but we have access to a small validation set with clean data. The metric $M$ here is evaluated on the clean validation set, and the surrogates $\ell_1, \ldots, \ell_K$ might be convex $l_p$ losses on the training data with different values of $p > 1$ to tune the noise robustness. In this case, the precise mathematical relationship $\psi$ between the validation metric and the surrogates is unknown.

**Example 3 (ML Fairness Problems).** For blackbox ML fairness metrics, good surrogates might be logistic losses on the positive and negative samples for different groups.

**Example 4 (Ranking Metrics).** Consider optimizing a ranking metric such as precision@$K$ for small validation set with clean data. The $\ell_1, \ldots, \ell_K$ might be convex $l_p$ losses on the training data with different values of $p > 1$ to tune the noise robustness. In this case, the precise mathematical relationship $\psi$ between the validation metric and the surrogates is unknown.

### 3.2. High-level Approach

Let $L := \{(\ell_1(\theta), \ldots, \ell_K(\theta)) \mid \theta \in \mathbb{R}^d\}$ be the set of feasible surrogate profiles. We then seek to approximate (1) by ignoring the slack $\epsilon$ and posing the problem as an optimization of $\psi$ over the $K$-dimensional set $L$:

$$\min_{\ell \in L} \psi(\ell). \quad (2)$$

Our high-level idea is to solve this re-formulated problem by applying **projected gradient descent** over $L$.

However, there are many challenges in implementing this idea. First, while each $\ell_k$ is convex, the space of feasible surrogates $L$ is not necessarily a convex set. Second, the function $\psi$ is unknown to us, and therefore we need to estimate gradients for $\psi$ with only access to the metric $M$ and the surrogates $\ell$. Third, we would need to implement projections onto the $K$-dimensional surrogate space without explicitly constructing this set.

### 4. Surrogate Projected Gradient Descent

We now explain how we address the above challenges.

#### 4.1. Convexifying the Surrogate Space

To turn (2) into a problem over a convex domain, we define the epigraph of the convex surrogate function profiles:

$$U := \{ \mathbf{u} \in \mathbb{R}^K_+ \mid \mathbf{u} \geq \ell(\theta) \text{ for some } \theta \in \mathbb{R}^d \}. \quad (3)$$

This relaxation preserves the optimizer for (2) because $\psi$ is monotonic and $U$ consists of upper bounds on surrogate profiles in $L$.

**Observation 1.** $U$ is a convex superset of $L$.

We then optimize $\psi$ over this $K$-dimensional convex set:

$$\min_{\mathbf{u} \in U} \psi(\mathbf{u}). \quad (4)$$

Next to estimate gradients without direct access to $\psi$, we measure changes in the $K$ surrogates $\ell(\cdot)$ and changes in the metric $M(\cdot)$ at different perturbations of $\theta^t$ and compute estimates of $\nabla \psi(\mathbf{u}^t)$ based on finite-differences or local linear interpolations. To compute projections without direct access to $U$, we formulate a convex optimization problem over the original parameters $\theta$, and show that this results in an over-constrained projection onto $U$.

#### 4.2. Projected Gradient Descent over $U$

We then perform projected gradient descent over $U$. We maintain iterates $\mathbf{u}^t$ in $U$, and at each step, (i) estimate the gradient of $\psi$ w.r.t. the $K$-dimensional point $\mathbf{u}^t$, (ii) perform a descent step:

$$\mathbf{u}^{t+1} = \mathbf{u}^t - \eta \nabla \psi(\mathbf{u}^t),$$

for some $\eta > 0$, and (iii) project $\mathbf{u}^{t+1}$ onto $U$ to get the next iterate $\mathbf{u}^{t+1}$.

In order to implement these steps without knowing $\psi$, we would need to implement projections onto $U$ and pose the problem as an optimization of $\psi$ over the $K$-dimensional convex set $L$.

Thus we maintain iterates $(\mathbf{u}^t, \theta^t)$ such that $\mathbf{u}^t = \ell(\theta^t)$, and execute the following at every iteration:

$$\mathbf{u}^{t+1} = \mathbf{u}^t - \eta \nabla \psi(\mathbf{u}^t; M, \ell),$$

$$(\mathbf{u}^{t+1}, \theta^{t+1}) = \text{proj}_{U}(\mathbf{u}^{t+1}; \ell).$$

Figure 1 gives a schematic description of the updates. The gradient computation takes the current $\theta^t$ as input and...
where we set up an optimization over \( \ell \), as we show below, advantage of the optimization problem being convex. More-

\[ L(u) = \frac{1}{2} \| u \|_2^2 + \sum_{i=1}^{K} \ell_i(u_i) \]

The space of surrogate profiles \( \mathcal{L} = \{ (\ell_1(\theta), \ell_2(\theta)) \mid \theta \in \mathbb{R}^d \} \) is a non-convex set (solid line), and its epigraph \( \mathcal{E} = \{ u \geq \ell \mid \ell \in \mathcal{L} \} \) is convex (shaded region). For the point \( u_a \) outside \( \mathcal{U} \), the solution \( u_a \) to (4) is the same as the exact projection \( \Pi(u_a) \) onto \( \mathcal{U} \). For the point \( u_b \) inside the set, the projection \( \Pi(u_b) \) is the same point \( u_b \), whereas the solution to (4) is any point \( u_b \) on the boundary that is less or equal to the exact projection in each coordinate, i.e. \( u_b \leq \Pi(u_b) \).

**4.3. Over-constrained Projection**

To implement the projection without explicit access to \( \mathcal{U} \), we set up an optimization over \( \theta \) by penalizing a clipped \( L_2 \)-distance between the surrogate profile \( \ell(\theta) \) and \( u^{t+1} \):

\[
\theta^{t+1} = \arg\min_{\theta \in \mathbb{R}^d} \| \ell(\theta) - u^{t+1} \|_2^2
\]

where \( (z)_+ := \max\{0, z\} \) is applied element-wise and \( \| \cdot \| \) is the \( L_2 \)-norm. Note that we penalize errors in only one direction (i.e., the errors where \( \ell_k(\theta) \geq u^{t+1}_k \)). This has the advantage of the optimization problem being convex. Moreover, as we show below, (4) results in an over-constrained projection: any solution \( u^{t+1} \) to (4) is feasible (i.e., is in \( \mathcal{U} \)), and for a monotonic \( \psi \), yields a \( \psi \)-value that is no worse than what we would get with an exact projection.

**Lemma 1.** Let \( u^+ \) be the exact projection of \( \hat{u}^{t+1} \in \mathbb{R}^+_d \) onto \( \mathcal{U} \). For any solution \( u^{t+1} \) to (4), we have \( u^{t+1} \leq u^+ \), and for a monotonic \( \psi \), \( \psi(u^{t+1}) \leq \psi(u^+) \).

**Algorithm 1** Surrogate Projected Gradient Descent

1. **Input:** Black-box metric \( M \), surrogate loss functions \( \ell_1, \ldots, \ell_K : \mathbb{R}^d \to \mathbb{R}^+ \), hyper-parameters: \( T, \eta \)
2. **Initialize** \( \theta^1 \in \mathbb{R}^d \)
3. **for** \( t = 1 \) **to** \( T \) **do**
   4. **Gradient estimate:** Obtain an estimate \( \hat{g}^t \) for gradient \( \nabla \psi(u^t) \) by invoking Algorithms 2 or 3 with inputs \( \theta^t \), \( M \) and \( \ell_1, \ldots, \ell_K \)
   5. **Gradient update:** \( \hat{u}^{t+1} = u^t - \eta \hat{g}^t \)
   6. **Over-constrained projection:** Solve:
      \[
      \theta^{t+1} = \arg\min_{\theta \in \mathbb{R}^d} \| \ell(\theta) - \hat{u}^{t+1} \|_2^2
      \]
      to accuracy \( O(\frac{1}{\eta T}) \) and set \( u^{t+1} = \ell(\theta^{t+1}) \)
7. **end for**

Problem (4) may not have a unique solution. For example, when \( \hat{u}^{t+1} \) is in the interior of \( \mathcal{U} \), the exact projection \( u^+ \) is the same as \( \hat{u}^{t+1} \), whereas the solutions to (4) are the points \( u \) on the boundary of \( \mathcal{U} \) with \( u \leq u^+ \) (see Figure 2). As \( \psi \) is monotonic, picking any of these solutions for the next iterate is sufficient for the algorithm’s convergence.

An outline of the projected gradient descent with this inexact projection is presented in Algorithm 1. One can interpret the algorithm as adaptively combining the \( K \) surrogates \( \ell_k \)’s to optimize the metric \( M \) (see Appendix C for the details).

**4.4. Convergence Guarantee**

We show convergence of Algorithm 1 to a stationary point of \( \psi(\ell(\cdot)) \). Since we probe \( M \) to estimate gradients for \( \psi \), the errors in the estimate would depend on how closely \( \psi(\ell(\cdot)) \) approximates \( M \), and in turn on the magnitude of the slack term \( \epsilon \). We assume here that the gradient estimation error \( \mathbb{E} \| \hat{g}^t - \nabla \psi(\ell(\theta^t)) \|_2^2 \) at each step \( t \) is bounded by \( \kappa_\epsilon \) that depends on the slack \( \epsilon \). In Section 5, we present gradient estimates that satisfy this condition.

**Theorem 2** (Convergence of Algorithm 1). Let \( M(\theta) = \psi(\ell(\theta)) + \epsilon(\theta) \), for a \( \psi \) that is monotonic, \( \beta \)-smooth and \( L \)-Lipschitz, and the worst-case slack \( \max_{\theta \in \mathbb{R}^d} |\epsilon(\theta)| \) is the minimum among all such decompositions of \( M \).

Suppose each \( \ell_k \) is \( \gamma \)-smooth and \( \Phi \)-Lipschitz in \( \theta \) with \( \|\ell(\theta)\| \leq G, \forall \theta \). Suppose the gradient estimates \( \hat{g}^t \) satisfy \( \mathbb{E} \| \hat{g}^t - \nabla \psi(\ell(\theta^t)) \|_2^2 \leq \kappa_\epsilon, \forall t \in [T] \) and the projection step satisfies \( \| \ell(\theta^{t+1}) - \hat{u}^{t+1} \|_2^2 \leq \min_{\theta \in \mathbb{R}^d} \| \ell(\theta) - \hat{u}^{t+1} \|_2^2 + O(\frac{1}{T}) \), \( \forall t \in [T] \). Set stepsize \( \eta = \frac{1}{2T} \).

Then Algorithm 1 converges to an approximate stationary point of \( \psi(\ell(\cdot)) \):

\[
\min_{1 \leq t \leq T} \mathbb{E} \| \nabla \psi(\ell(\theta^t)) \|_2^2 \leq C \left( \frac{\beta}{\sqrt{T}} + \sqrt{\kappa_\epsilon} + \sqrt{LK\epsilon} \right),
\]

where the expectation is over the randomness in the gradient estimates, and \( C = O(KL(\gamma(G + \frac{1}{T}) + \Phi^2)) \).
We now address the issue of estimating the gradient value of surrogate loss for a Gaussian distribution, and evaluate the difference between the scores surrogates for Gaussian vectors labels the evaluation metric overload notation and use the model \( f \) and metric \( \mathcal{M} \). Then we exploit the smoothness of the surrogates \( \ell \) to show that this result translates to the algorithm converging to an approximate stationary point of the metric \( \mathcal{M} \).

The proof of Theorem 2 proceeds in two parts. We first show that the algorithm converges to an approximate stationary point of \( \psi \) over \( \mathcal{U} \). For this, we extend recent results of Ghadimi et al. (2016) on convergence of projected gradient descent for smooth non-convex objectives. We then exploit the smoothness of the surrogates \( \ell \) to show that this result translates to the algorithm converging to an approximate stationary point of \( \psi^i(\ell(\cdot)) \) w.r.t. \( \theta \).

Remark 2 (Prior convergence results). A key difference between our analysis and prior works on zeroth-order gradient methods (Duchi et al., 2015; Ghadimi et al., 2016; Nesterov and Spokoiny, 2017) is that we do not directly optimize the given objective over the space of parameters \( \theta \), and instead perform an optimization over a relaxed surrogate space \( \mathcal{U} \) that is not directly specified, and so do using inexact projections and approximate gradient estimates.

5. Gradient Estimation Techniques

We now address the issue of estimating the gradient \( \nabla \psi^i(\ell(\cdot)) \) at a given \( \ell(\theta_i) \) without explicit access to \( \psi \). We provide an algorithm based on finite-differences, and another based on local linear interpolations. We also show error bounds for these algorithms, i.e., bound the errors \( \kappa_i \) in Theorem 2.

5.1. Finite Differences

We first consider the case where both the surrogates \( \ell \) and metric \( M \) are evaluated on the same sample. Let \( f_0 := [f_0(x_1), \ldots, f_0(x_n)]^T \in \mathbb{R}^n \) denote the scores of the model \( \theta \) computed on the \( n \) training examples. We overload notation and use \( M(f_0, y) \) to denote the value of the evaluation metric \( M \) on the model scores \( f_0 \in \mathbb{R}^n \) and labels \( y \in \mathcal{Y}^n \). Similarly, we use \( \ell_k(f_0, y) \) to denote the value of surrogate loss \( \ell_k \) on \( f_0 \) and \( y \).

We present our method in Algorithm 2. We adopt a standard finite-difference gradient estimate (Nesterov and Spokoiny, 2017), which requires us to perturb the surrogates \( \ell \) with random Gaussian vectors \( Z_1, \ldots, Z_m \sim \mathcal{N}(0, \mathbf{I}_K) \), evaluate \( \psi \) at the perturbed surrogate profiles, and calculate

\[
\frac{1}{m} \sum_{j=1}^{m} \nabla \psi(\ell(f_0, y) + \sigma Z_j) - \psi(\ell(f_0, y)),
\]

for \( \sigma > 0 \). In our case, we cannot directly perturb the surrogates \( \ell \) and evaluate changes in \( \psi \). Instead, we perturb the scores \( f_0 \) so that the corresponding changes in \( \ell \) follows a Gaussian distribution, and evaluate the difference between the metric \( M \) at the original and perturbed scores. This is possible, for example, when each \( \ell_k(f_0, y) \) is an average of point-wise losses \( \phi_k(y, f_0(x_i)) \) on different subsets of the data, for some invertible function \( \phi_k : \mathbb{R} \rightarrow \mathbb{R} \), in which case, it is easy to compute the right amount of perturbation to the scores \( f_0 \) to produce the desired perturbation in \( \ell_k \).

Lemma 3 (Finite difference estimate). Let \( M \) be as defined in Theorem 2 and \( |\varepsilon(\theta)| \leq \varepsilon, \forall \theta \). Let \( \hat{g} \) be returned by Algorithm 2 for a given \( \theta_i \), \( m \) perturbations and \( \sigma = \frac{\sqrt{2}}{\sqrt{K} \beta^2} \).

\[
\mathbb{E} \left[ \| \hat{g} - \nabla \psi(\ell(\theta_i)) \|^2 \right] \leq O \left( \frac{L^2 K}{m} + \varepsilon K^2 \beta^2 \right),
\]

where the expectation is over the random perturbations.

This gives a bound on \( \kappa_i \) in Theorem 2 when Algorithm 2 is used for gradient estimates. Note the error depends on the slack magnitude \( \varepsilon \), and decreases with more perturbations.

5.2. Local Linear Interpolations

The finite-difference approach is not applicable to settings where the metric is evaluated on a validation sample but the surrogates are evaluated on training examples (as in Example 2), or where finding the right amount of perturbation on the scores is difficult. For such cases we present a local linear interpolation based approach in Algorithm 3, where we perturb the model parameters \( \theta \) instead of the scores.

We use the fact that a smooth function \( \psi \) can be locally approximated by a linear function, and estimate the gradient of \( \psi \) of at \( \ell(\theta) \) by perturbing \( \theta \), measuring the corresponding differences in the surrogates \( \ell \) and the metric \( M \), and fitting a linear function from the surrogate differences to

### Algorithm 2 Finite-difference Gradient Estimate

1. **Input**: \( \theta^i \in \mathbb{R}^d, M, \ell_1, \ldots, \ell_K \)
2. **Hyper-parameters**: Num of perturbations \( m, \sigma \)
3. Draw \( Z_1, \ldots, Z_m \sim \mathcal{N}(0, \mathbf{I}_K) \)
4. Find \( \Delta_j \in \mathbb{R}^n \) s.t. \( \ell(f_0 + \Delta_j, y) = \ell(f_0, y) + \sigma Z_j \), for \( j = 1, \ldots, m \)
5. \( \hat{g} = \frac{1}{m} \sum_{j=1}^{m} M(f_0 + \Delta_j, y) - M(f_0, y) \)
6. **Output**: \( \hat{g} \)

### Algorithm 3 Linear Interpolation Gradient Estimate

1. **Input**: \( \theta^i \in \mathbb{R}^d, M, \ell_1, \ldots, \ell_K \)
2. **Hyper-parameters**: Num of perturbations \( m, \sigma \)
3. Draw \( Z_1, \ldots, Z_m \sim \mathcal{N}(0, \mathbf{I}_d) \)
4. \( H_m = \ell(\theta + \sigma Z_1) - \ell(\theta + \sigma Z_2), j = 1, \ldots, m \)
5. \( M_m = M(\theta + \sigma Z_1) - M(\theta + \sigma Z_2), j = 1, \ldots, m \)
6. \( \hat{g} = \arg\min_{g \in \mathbb{R}^K} \| Hg - M_m \|^2 \)
7. **Output**: \( \hat{g} \)
the metric differences. Specifically, for \( d \) model parameters, we draw two independent sets of \( d \)-dimensional Gaussian perturbations \( Z_1^1, \ldots, Z_1^m, Z_2^1, \ldots, Z_2^m \sim \mathcal{N}(0, I_d) \), and return a linear fit from \( H = \left[ \ell(\theta + \sigma Z_1^1) - \ell(\theta + \sigma Z_2^1) \right]_{j=1}^m \) to \( M = [M(\theta + \sigma Z_1^1) - M(\theta + \sigma Z_2^1)]_{j=1}^m \).

**Lemma 4** (Linear interpolation estimate). Let \( M \) be defined as in Theorem 2 and \( |\epsilon(\theta)| \leq \epsilon, \forall \theta \). Assume each \( \ell_k \) is \( \Phi \)-Lipschitz in \( \theta \) w.r.t. the \( L_\infty \)-norm, and \( |\ell(\theta)| \leq G, \forall \theta \). Suppose for a given \( \theta', \sigma \) and perturbation count \( m \), the expected covariance matrix for the left-hand-side of the linear system \( H \) is well-conditioned, and has the smallest singular value \( \lambda_{\min}(\sum_{i=1}^m E[H_i H_i^T]) = \mathcal{O}(m^2 \Phi^2) \). Then setting \( \sigma = \tilde{O} \left( G^{1/3} \frac{1}{\epsilon^2} \right) \) and \( m = \tilde{O} \left( \frac{G^4 K^9 \beta^2}{\epsilon^2} \right) \), Algorithm 3 returns w.h.p. (over draws of random perturbations) a gradient estimate \( \tilde{g} \) that satisfies:

\[
\| \tilde{g} - \nabla \psi(\ell'(\theta')) \|^2 \leq \tilde{O} \left( G^{1/3} \frac{1}{\epsilon^2} K^3 \beta^{2/3} \right).
\]

We show in Appendix A.5 how this high probability statement can then be used to derive a bound on the expected errors \( \kappa_\epsilon \), in Theorem 2. Prior works provide error bounds on a similar gradient estimate under an assumption that the perturbation matrix \( H \) can be chosen to be invertible (Conn et al., 2008; 2009; Berahas et al., 2019). In our case, however, \( H \) is not chosen explicitly, but instead contains measurements of changes in surrogates for random perturbations on \( \theta \). Hence to show an error bound, we need a slightly subtle condition on the correlation structure of the surrogates (that essentially says the variance of the perturbed surrogates are large enough and the rates are not strongly correlated with each other), which we express as a condition on the smallest singular value of the covariance of \( H \).

5.3. Handling Non-smooth Metrics

For \( \psi \) that is non-smooth and Lipschitz, we extend the finite difference gradient estimate in Section 5.1 with a two-step perturbation. We draw two sets of Gaussian random vectors \( Z_1^1, \ldots, Z_1^m, Z_2^1, \ldots, Z_2^m \sim \mathcal{N}(0, I_K) \) and calculate

\[
1 \sum_{m=1}^m \psi(\ell(\mathbf{f}_0, y) + \sigma_1 Z_1^1 + \sigma_2 Z_2^1) - \psi(\ell(\mathbf{f}_0, y) + \sigma_1 Z_1^1)
\]

for \( \sigma_1, \sigma_2 > 0 \), where we perturb \( \ell \) by perturbing the scores \( \mathbf{f}_0 \). This approach computes a finite-difference gradient estimate for a smooth approximation to the original \( \psi \), given by \( \psi_{\sigma_1}(u) := E[\psi(u + \sigma_1 Z_1)] \), where \( Z_1 \sim \mathcal{N}(0, I_K) \). We provide error bounds in Appendix B by building on recent work by Duchi et al. (2015), and discuss asymptotic convergence of Algorithm 1 as \( \sigma_1 \to 0 \).

6. Experiments

We present experiments to show the proposed approach, Algorithm 1, is able to perform as well as methods that take advantage of a metric’s form where available, and is also able to provide gains for metrics that are truly a black-box. We consider a simulated classification task, a fair classification task with noisy features, a ranking task and classification tasks with proxy and noisy labels. The datasets we use are listed in Table 1.

We use the linear interpolation approach in Algorithm 3 for estimating gradients, as this is the most practical among the proposed estimation methods, and applicable when the surrogates and metrics are evaluated on different samples. We train linear models in all experiments, and tune hyper-parameters such as step sizes and the perturbation parameter \( \sigma \) for gradient estimation using a held-out validation set. We run the projected gradient descent with 250 outer iterations and 1000 perturbations. For the projection step, we run 100 iterations of Adagrad. See Appendix D for more details and a discussion on perturbations. TensorFlow code has been made available.\(^1\)

### 6.1. Optimizing G-mean on Simulated Data

<table>
<thead>
<tr>
<th>Dataset</th>
<th>#instances</th>
<th>#features</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulated</td>
<td>1000</td>
<td>0.498</td>
<td>0.344</td>
</tr>
</tbody>
</table>

\(^1\)https://github.com/google-research/google-research/tree/master/adaptive_surrogates
We use four fairness datasets: (1) COMPAS, where the goal is to predict recidivism with gender as the protected attribute (Angwin et al., 2016); (2) Adult, where the goal is to predict if a person’s income is more than 50K/year, and we take gender as the protected group (Blake and Merz, 1998); (3) Credit Default, where the task is to predict whether a customer would default on his/her credit card payment, and we take gender as the protected group (Blake and Merz, 1998); (4) Business Entity Resolution, a proprietary dataset from a large internet services company, where the goal is to predict whether a pair of business descriptions refer to identical businesses, and we consider non-chain businesses as protected. In each case, we split the data into train-validation-test sets in the ratio 4/9 : 2/9 : 1/3.

6.2. Macro F-measure with Noisy Features

For this experiment we consider training a classifier with fairness goals defined on binary protected attributes. We seek to maximize the average F-measure across the groups:

$$\text{Macro } F_1 = \frac{1}{2} \sum_{G \in \{0,1\}} \frac{2 \times \text{Precision}_G \times \text{Recall}_G}{\text{Precision}_G + \text{Recall}_G},$$

where Precision$_G$ and Recall$_G$ are the precision and recall on protected group $G$. Optimizing a sum of F-measures is harder than optimizing the binary F-measure because the summation destroys its pseudo-convexity property (Narasimhan et al., 2019).

We use four fairness datasets: (1) COMPAS, where the goal is to predict recidivism with gender as the protected attribute (Angwin et al., 2016); (2) Adult, where the goal is to predict if a person’s income is more than 50K/year, and we take gender as the protected group (Blake and Merz, 1998); (3) Credit Default, where the task is to predict whether a customer would default on his/her credit card payment, and we take gender as the protected group (Blake and Merz, 1998); (4) Business Entity Resolution, a proprietary dataset from a large internet services company, where the goal is to predict whether a pair of business descriptions refer to identical businesses, and we consider non-chain businesses as protected. In each case, we split the data into train-validation-test sets in the ratio 4/9 : 2/9 : 1/3.

Training with no noise. The first set of experiments tests if the proposed approach is able to match the performance of existing methods that are customized to optimize the macro F-measure. We compare against (i) plain logistic regression method, (ii) a plug-in or post-shift method that tunes a threshold on the logistic regression model to maximize the F-measure (Koyejo et al., 2014; Narasimhan et al., 2014), (iii) an approach that optimizes a continuous relaxation to the F-measure that replaces the indicators with the hinge loss (see e.g. Zhao et al. (2019a)), and (iv) the recent “generalized rates” approach of Narasimhan et al. (2019) for optimizing metrics that are a sum of ratios. We apply our approach using four surrogate losses, each one is the hinge loss averaged over either the positive or negative examples, calculated separately for each of the two groups. As seen in Table 3, despite having only black-box access to the metric, the proposed approach is competitive with the other methods that are directly tailored to optimize the macro F-measure.

Training with noisy features. The second set of experiments evaluates the performance of these methods when the training set has noisy features for just one of the groups, while the smaller validation set contains clean features. We use our approach to adaptively combine the same four surrogate losses computed on the noisy training set to best optimize the macro F-measure on the clean validation set.

We chose a certain fraction of the examples at random from one of the groups, which we refer to as group 0, and for these examples, we add Gaussian noise to the real features (with mean 0 and the same standard deviation as the feature), and flip the binary features with probability 0.9. Figure 4 shows the test F-measure for the different methods with varying fraction of noisy examples in group 0. Except for logistic regression, all other methods have access to the validation set: post-shift uses the validation set to tune a threshold on the logistic regression model; the RelaxedFM and GenRates method optimize their loss on the training set, but pick the best model iterate using the validation set.

6.3. Ranking to Optimize PRBEP

We next consider a ranking task, where the goal is to learn a scoring function $f$ that maximizes the precision-recall break-even point (PRBEP), i.e. yields maximum precision at the
threshold where precision and recall are equal. PRBEP is a special case of Precision@$K$ when $K$ is set to the number of positive examples in the dataset. For this task, we experiment with the KDD Cup 2008 breast cancer detection data set (Rao et al., 2008) popularly used in this literature (Kar et al., 2015; Mackey et al., 2018). We randomly split this dataset 60/20/20 for training, validation, and test.

Since the break-even point for a dataset is not known beforehand, we use surrogates that approximate precision at different recall thresholds $\tau$. We use the quantile-based surrogate losses of Mackey et al. (2018) with $\tau = 0.25, 0.5, 0.75$. As a comparison, we optimize the avg-precision@$K$ surrogate provided by Kar et al. (2015). As seen in Table 4, the proposed approach is able to learn a better training loss by combining the three quantile surrogates, and yields the best PRBEP on the both the training and test sets.

### 6.4. Classification with Proxy Labels

Next, we consider classification tasks where the training labels are proxies for the true labels, but the validation data has the true labels. We seek to minimize the classification error on the validation set by combining hinge loss surrogates evaluated separately on the positive and negative training examples. While the theory requires convex losses, we experiment with also running the algorithm with non-convex sigmoid losses as surrogates.

For the Adult data, we predict whether a candidate’s gender is female, and take the marital-status-wife feature as the proxy label. For the Business Entity Resolution data, we predict whether a pair of business descriptions refer to the same business, and use the has-same-phone-number feature as a proxy label.

We compare with a logistic regression model trained with the proxy labels and a post-shift method that corrects the logistic regression threshold to minimize classification error on the validation data. In the results shown in 5, as expected logistic regression yields the highest test error. On Adult, both variants of the proposed method are better than Post-Shift. On Business, the proposed method performs slightly worse than PostShift when run with hinge surrogates, but yields notable improvements when run with sigmoid surrogates, which are tighter relaxations to the true errors.
Table 6. Validation and test G-mean on Adult dataset with noisy training labels, averaged over 5 trials. The proposed method was run with both hinge and sigmoid surrogates. Lower is better.

<table>
<thead>
<tr>
<th></th>
<th>LogReg</th>
<th>PostShift</th>
<th>MOEW</th>
<th>Hinge</th>
<th>Sigmoid</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Val</strong></td>
<td>0.482</td>
<td>0.178</td>
<td>0.199</td>
<td>0.187</td>
<td><strong>0.165</strong></td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>0.437</td>
<td>0.184</td>
<td>0.223</td>
<td>0.186</td>
<td><strong>0.176</strong></td>
</tr>
</tbody>
</table>

6.5. Optimizing G-mean with Noisy Labels

We finally consider classification tasks where the training labels are noisy, but we have access to a validation sample with true labels. We experiment with the Adult dataset, with the goal of predicting if a person’s income is more than 50K/year. We hold out 1% of the training data for validation, and in remaining data, we randomly pick 30% of the positive labels and flip them to negative. We seek to minimize the G-mean metric given by $1 - \sqrt{TPR \times TNR}$ on the validation set. We apply our approach using ten surrogate losses, each one is the hinge loss averaged over either the positive or negative examples, calculated separately for five groups of examples: male, female, black, white and private-workforce. We also applied our approach using sigmoid surrogates averaged over the same ten subsets.

We compare with a logistic regression model trained with noisy labels and a post-shift method that corrects the logistic regression threshold to minimize G-mean on the validation data. We also compare with a grid-search-based variant of the metric-optimized example weights (MOEW) approach of Zhao et al. (2019b). MOEW optimizes a black-box metric by learning a weighted training objective, where the weights on the individual examples are trained to minimize a given metric on the validation set. We model the example weights as a linear function of a 2-dimensional feature embedding and the labels, and tune the parameters of the weighting function using an exhaustive grid search.

The results are shown in Table 6. The proposed method with sigmoid surrogates yields the lowest G-mean on the validation and test sets, with post-shift coming in second. The sigmoid surrogates, being tighter approximation to the training errors, once again yield better results than the hinge surrogates. In Appendix D, we provide further details and an additional experiment with simulated data.

7. Discussion

There is currently a lot of interest in training models with better alignment with evaluation metrics. Here, we have investigated a simple method that directly estimates only the needed gradients for gradient descent training, and does not require assuming a parametric form. This simplicity enabled us to provide rigorous theoretical guarantees. Experimentally, our approach was as good as strategies that take advantage of a metric’s known mathematical form. In our experiments imitating real use cases for our method, we obtained notable gains over exiting baselines for classification with group-dependent noise, and for black-box ranking. For the experiments with proxy and noisy labels, however, we found the post-shifting approach to be competitive, with the proposed method yielding gains over post-shift when run with tight surrogate approximations to classification errors.

Post-shift is a strong baseline – in theory, for many metrics it is optimal to simply post-shift the Bayes class probability model $P(y = 1|x)$ with a suitable threshold $\beta$ (Koyejo et al., 2014; Yan et al., 2018). Post-shift only has one degree of freedom, which limits it, but also enables choosing $\beta$ to directly optimize the true metric. In contrast, our method acts through surrogate losses to optimize the target metric. We argue that post-shift should be a required baseline for experiments on custom metric optimization.

We look forward to seeing further theoretical analysis for handling black-box metrics, and further experimentation comparing methods with fewer but smarter parameters to those with more flexible modeling.

Acknowledgements

We thank Andrew Cotter for several helpful discussions.

References


Optimizing Black-box Metrics with Adaptive Surrogates


