A NEAR-OPTIMAL ALGORITHM FOR DEBIASING TRAINED MACHINE LEARNING MODELS

Anonymous authors
Paper under double-blind review

ABSTRACT

We present an efficient and scalable algorithm for debiasing trained models, including deep neural networks (DNNs), which we prove to be near-optimal by bounding its excess Bayes risk. Unlike previous black-box reduction methods to cost-sensitive classification rules, the proposed algorithm operates on models that have been trained without having to retrain the model. Furthermore, as the algorithm is based on projected stochastic gradient descent (SGD), it is particularly attractive for deep learning applications. We empirically validate the proposed algorithm on standard benchmark datasets across both classical algorithms and modern DNN architectures and demonstrate that it outperforms previous post-processing approaches for unbiased classification.

1 INTRODUCTION

Machine learning is increasingly applied to critical decisions which can have a lasting impact on individual lives, such as for credit lending (Bruckner, 2018), medical applications (Deo, 2015), and criminal justice (Brennan et al., 2009). Consequently, it is imperative to understand and improve the degree of bias of such automated decision-making.

Unfortunately, despite the fact that bias (or "fairness") is a central concept in our society today, it is difficult to define it in precise terms. In fact, as people perceive ethical matters differently depending on a plethora of factors including geographical location or culture (Awad et al., 2018), no universally-agreed upon definition for bias exists. Moreover, the definition of bias may depend on the application and might even be ignored in favor of accuracy when the stakes are high, such as in medical diagnosis (Kleinberg et al., 2017; Ingold and Soper, 2016). As such, it is not surprising that several definitions of "unbiased classification" have been introduced. These include statistical parity (Dwork et al., 2012; Zafar et al., 2017a), equality of opportunity (Hardt et al., 2016), and equalized odds (Hardt et al., 2016; Kleinberg et al., 2017). Unfortunately, such definitions are not generally compatible (Chouldechova, 2017) and some might even be in conflict with calibration (Kleinberg et al., 2017). In addition, because fairness is a societal concept, it does not necessarily translate into a statistical criteria (Chouldechova, 2017; Dixon et al., 2018).

Conditional statistical parity Let $\mathcal{X}$ be an instance space and let $\mathcal{Y} = \{0, 1\}$ be the target set in a standard binary classification problem. In the fair classification setting, we may further assume the existence of a (possibly randomized) sensitive attribute $1_S : \mathcal{X} \to \{0, 1\}$, where $1_S(x)$ indicates if an instance $x \in \mathcal{X}$ belongs to some sensitive class $S \subseteq \mathcal{X}$. For example, $\mathcal{X}$ might correspond to the set of job applicants while S are the female applicants. Here, the sensitive attribute can be randomized if, for instance, the gender of an applicant is not a deterministic function of the full instance $x \in \mathcal{X}$ (e.g. number of publications, years of experience, ...etc). Then, a general theme among common definitions of bias is to fix a partitioning of the instance space $\mathcal{X} = \cup_k X_k$ where $X_{k_1} \cap X_{k_2} = \emptyset$ for $k_1 \neq k_2$ and require a balanced representation of the sensitive class within some or all of the subsets X_k (i.e., the *groups*). We note that the groups X_k are different from the sensitive class S. If the sensitive attribute is e.g. gender, the groups can be based on race, age, etc., but not on gender. In the latter case, the goal is to make sure that females and males are treated equally within each group (e.g. males and females are treated the same within every racial group, not just overall). This property is well-captured through the notion of statistical parity (Corbett-Davies et al., 2017; Dwork et al., 2012; Zafar et al., 2017a; Mehrabi et al., 2019):

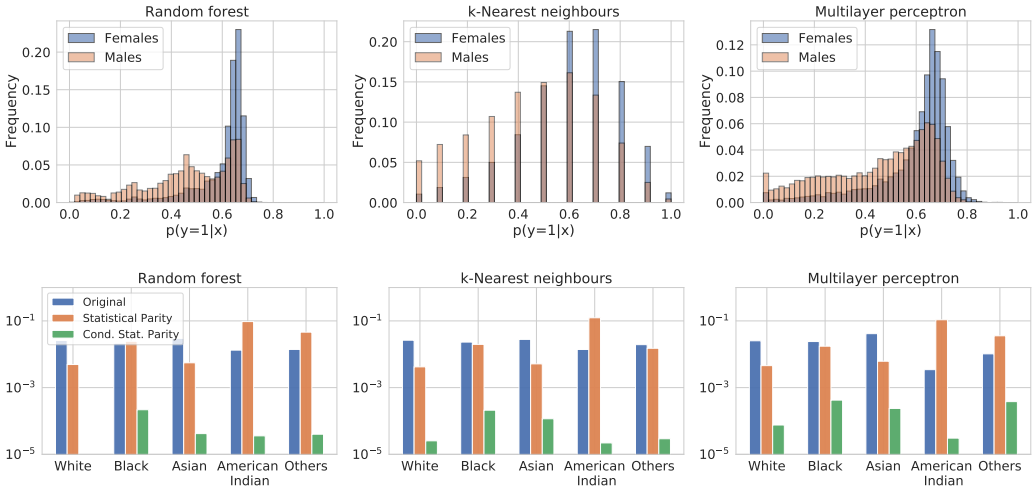


Figure 1: **Top:** Histogram of classifiers' predictions on both subpopulations, demonstrating a clear gender bias in all cases. **Bottom:** The bias defined as the absolute value of the covariance between gender and the classifier's prediction, both as binary random variables, before and after applying the proposed algorithm. Blue bars show the results of the unmodified classifier, orange bars show the results of optimizing for statistical parity with no regard for demographic information. Finally, green bars are the results of applying conditional statistical parity within every racial group.

Definition 1 (Conditional Statistical Parity)**.** *Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \{0, 1\}$ be random variables. Let $C(\boldsymbol{a}, \boldsymbol{b}) \doteq \mathbb{E}[\boldsymbol{a} \cdot \boldsymbol{b}] - \mathbb{E}[\boldsymbol{a}] \cdot \mathbb{E}[\boldsymbol{b}]$ be their covariance, and $C(\boldsymbol{a}, \boldsymbol{b} \,|\, \boldsymbol{c})$ their covariance conditioned on $\boldsymbol{c}$:*

$$C(\boldsymbol{a}, \boldsymbol{b} \mid \boldsymbol{c} = c) = \mathbb{E}[\boldsymbol{a} \cdot \boldsymbol{b} \,|\, \boldsymbol{c} = c] - \mathbb{E}[\boldsymbol{a} \,|\, \boldsymbol{c} = c] \cdot \mathbb{E}[\boldsymbol{b} \,|\, \boldsymbol{c} = c].$$

A classifier $f : \mathcal{X} \to \{0, 1\}$ satisfies ϵ conditional statistical parity in some group $X_k \subseteq \mathcal{X}$ with respect to a sensitive class S if $\left|C\big(f(\boldsymbol{x}),\, 1_S(\boldsymbol{x}) \,|\, \boldsymbol{x} \in X_k\big)\right| \leq \epsilon$. A classifier f satisfies ϵ conditional statistical parity with respect to S across all groups $\{X_k\}_{k=1,2,\ldots,K}$ if it satisfies ϵ conditional statistical parity in each X_k.

To motivate and further clarify the definition, we showcase the empirical results on the Adult benchmark dataset (Blake and Merz, 1998) in Figure 1. When tasked with predicting whether the income of individuals is above \$50K per year, all considered classifiers exhibit gender-related bias. One way of removing such bias is to enforce statistical parity across genders. Crucially, however, without *conditional* statistical parity, different demographic groups may experience different outcomes. In fact, gender bias can actually *increase* in some minority groups after enforcing statistical parity. Applying our algorithm which enforces *conditional* statistical parity removes this bias (green bars).

Our main contribution in this paper is to present a near-optimal recipe for debiasing machine learning models, including deep neural networks, according to Definition 1. Specifically, we formulate the task of debiasing learned models as a regularized optimization problem. The problem can then be solved efficiently using the projected SGD method, where the projection step is a simple thresholding rule. We show how the algorithm produces thresholding rules with randomization near the thresholds, where the width of randomization is controlled by the regularization parameter. In addition, we show that randomization near the threshold is indeed necessary for Bayes risk consistency.

Statement of Contribution

1. We derive a near-optimal post-processing algorithm for debiasing learned models. We motivate the algorithm via an impossibility result, which quantifies the tradeoff between accuracy and fairness across multiple demographic groups (Section 3).
2. We prove theoretical guarantees for the proposed algorithm, including an explicit bound on its Bayes excess risk (Section 4).
3. We empirically validate the proposed algorithm on benchmark datasets and across both classical algorithms and modern DNN architectures. Our experiments demonstrate that the proposed algorithm significantly outperforms previous post-processing methods (Section 5).

2 RELATED WORK

Algorithms for fair machine learning can be broadly classified into three groups: (1) pre-processing methods, (2) in-processing methods, and (3) post-processing methods (Zafar et al., 2019).

Preprocessing algorithms transform the data into a different representation such that any classifier trained on it will not exhibit bias. This includes methods for learning a fair representation (Zemel et al., 2013; Lum and Johndrow, 2016; Bolukbasi et al., 2016; Calmon et al., 2017; Madras et al., 2018; Kamiran and Calders, 2012), label manipulation (Kamiran and Calders, 2009), data augmentation (Dixon et al., 2018), or disentanglement (Locatello et al., 2019). On the other hand, in-processing methods constrain the behavior of learning algorithms in order to control bias. This includes methods based on adversarial learning (Zhang et al., 2018) and constraint-based classification, such as by incorporating constrains on the decision margin (Zafar et al., 2019) or features (Grgić-Hlača et al., 2018). Agarwal et al. (2018) showed that the task of learning an unbiased classifier could be reduced to a *sequence* of cost-sensitive classification problems, which could be applied to any *black-box* classifier. One caveat of the latter approach is that it requires solving a linear program (LP) and retraining classifiers, such as neural networks, *many* times before convergence.

The algorithm we propose in this paper is a post-processing method, which can be justified theoretically (Corbett-Davies et al., 2017; Hardt et al., 2016; Menon and Williamson, 2018; Celis et al., 2019). Fish et al. (2016) and Woodworth et al. (2017) fall under this category. However, the former only provides generalization guarantees without consistency results and does not describe how the thresholds can be learned, while the latter proposes a two-stage approach that requires changes to the original training algorithm. In contrast, our algorithm is Bayes consistent and does not alter the original classification method. In Celis et al. (2019) and Menon and Williamson (2018), instance-dependent thresholding rules are also learned. However, our algorithm also learns to *randomize* around the threshold (Figure 2(a)) and this randomization is *key* to our algorithm both theoretically as well as experimentally (Appendix D and Section 5). Hardt et al. (2016) learns a randomized post-processing rule but our proposed algorithm outperforms it in all of our experiments (Section 5).

Woodworth et al. (2017) showed that the post-processing approach can, sometimes, be highly sub-optimal. Nevertheless, the latter result does not contradict the statement that our post-processing rule is near-optimal because we assume that the original classifier outputs a monotone transformation of some approximation to the posterior probability $p(\mathbf{y} = 1 \mid \mathbf{x})$ (e.g. margin or softmax output) whereas Woodworth et al. (2017) assumed in their construction that the post-processing rule had access to the binary predictions only. We argue that the proposed algorithm has distinct advantages, particularly for deep neural networks (DNNs). First, stochastic convex optimization methods are well-understood and can scale well to massive amounts of data (Bottou, 2010), which is often the case in deep learning today. Second, the guarantees provided by our algorithm hold w.r.t. the *binary* predictions instead of using a proxy, such as the margin as in some previous works (Zafar et al., 2017b; 2019). Third, unlike previous reduction methods to cost-sensitive classification rules that would require retraining a deep neural network several times until convergence (Agarwal et al., 2018), which can be prohibitively expensive, our algorithm operates on learned models that are trained once and does not require retraining.

Besides developing algorithms for fair classification, several recent works focused on other related aspects, such as proposing new definitions for fairness; e.g. demographic parity (Dwork et al., 2012; Mehrabi et al., 2019), equalized odds (Hardt et al., 2016), equality of opportunity/disparate mistreatment (Zafar et al., 2017a; Hardt et al., 2016), and individual fairness (Dwork et al., 2012). Recent works have also established several impossibility results related to fair classification, such as Kleinberg et al. (2017); Chouldechova (2017). In our case, we derive a new impossibility result that holds for *any* deterministic binary classifier, which highlights that the groups X_k (see Section 1) when defining fairness have to be known *in advance*.

3 NEAR-OPTIMAL ALGORITHM FOR CONDITIONAL STATISTICAL PARITY

Notation We reserve boldface letters for random variables (e.g. $\mathbf{x}$), small letters for instances (e.g. x), capital letters for sets (e.g. X), and calligraphic typeface for universal sets (e.g. the instance space $\mathcal{X}$). Given a set S, $1_S(x) \in \{0, 1\}$ is the characteristic function indicating whether $x \in S$. We denote by $[n]$ the set of integers $\{1, \ldots, n\}$ and $[x]^+ = \max\{0, x\}$.

Algorithm Given a classifier $f : \mathcal{X} \to [-1, +1]$ our goal is to post-process the predictions made by f[1] in order to control the bias with respect to a sensitive attribute $1_S : \mathcal{X} \to \{0, 1\}$ and across a fixed set of pairwise disjoint groups $X_1, \ldots, X_K \subseteq \mathcal{X}$ as in Definition 1. To this end, instead of outputing the result of f directly, we consider *randomized prediction rules* of the form

$$\tilde{h} : \mathcal{X} \times \{1, 2, \ldots, K\} \times \{0, 1\} \times [-1,\, 1] \to \{0, 1\},$$

where $\tilde{h}(\mathbf{x})$ represents the probability of predicting the positive class given (i) instance $\mathbf{x} \in \mathcal{X}$, (ii) group X_k, (iii) sensitive attribute $1_S(\mathbf{x})$, and (iv) classifier's output $f(\mathbf{x})$.

As shown in Appendix C, for post-processing rule $\tilde{h}(x) \in [0,\, 1]$, and for each group $X_k \subseteq \mathcal{X}$, the fairness constraint in Definition 1 can be written as $|\mathbb{E}_{\mathbf{x}}[(1_S(\mathbf{x}) - \rho_k)\, \tilde{h}(\mathbf{x}) | \mathbf{x} \in X_k] \;\leq\; \epsilon$, where $\rho_k = \mathbb{E}_{\mathbf{x}}[1_S(\mathbf{x}) \,|\, \mathbf{x} \in X_k]$. On the other hand, minimizing the probability of altering the predictions of the original classifier can be achieved by maximizing the inner product $\mathbb{E}_{\mathbf{x}}[\tilde{h}(\mathbf{x}) \cdot f(\mathbf{x})]$. Instead of optimizing this quantity directly, which would lead to a pure thresholding rule, we minimize the *regularized* objective: $(\gamma/2)\mathbb{E}_{\mathbf{x}}[\tilde{h}(\mathbf{x})^2] - \mathbb{E}_{\mathbf{x}}[\tilde{h}(\mathbf{x}) \cdot f(\mathbf{x})]$. This regularization leads to randomization around the threshold, which we show to be critical, both theoretically (Section 4) and experimentally (Section 5). Using Lagrange duality we show that the solution reduces to the update rules in Equation 2 with optimization variables $\{\lambda_k, \mu_k\}_{k \in [K]}$ and the corresponding predictor which outputs $+1$ for group X_k with probability $\tilde{h}(x)$ is given by

$$\tilde{h}(x) = \begin{cases} 0, & f(x) \leq (\lambda_k - \mu_k) z_k(x) \\ (f(x) - (\lambda_k - \mu_k) z(x))/\gamma, & (\lambda_k - \mu_k) z_k(x) \leq f(x) \leq (\lambda_k - \mu_k) z_k(x) + \gamma \\ 1, & f(x) \geq (\lambda_k - \mu_k) z_k(x) + \gamma \end{cases} \tag{1}$$

where ξ_γ is given by Eq. (3), $z_k(x) = 1_S(x) - \rho_k$. Here, $z_k(x)$ is a function that assigns different values inside and outside of the sensitive class, which allows the model to produce different thresholding rules.

Update rules To learn these parameters, one can apply the following update rules (Appendix C):

$$\begin{aligned} \lambda_{k(\mathbf{x})} &\leftarrow \max\Big\{0,\; \lambda_{k(\mathbf{x})} - \eta\Big(\epsilon + \frac{\partial}{\partial \lambda_{k(\mathbf{x})}} \xi_\gamma\big(f(\mathbf{x}) - (\lambda_{k(\mathbf{x})} - \mu_{k(\mathbf{x})}) \cdot z_{k(\mathbf{x})}(\mathbf{x})\big)\Big)\Big\} \\ \mu_{k(\mathbf{x})} &\leftarrow \max\Big\{0,\; \mu_{k(\mathbf{x})} - \eta\Big(\epsilon + \frac{\partial}{\partial \mu_{k(\mathbf{x})}} \xi_\gamma\big(f(\mathbf{x}) - (\lambda_{k(\mathbf{x})} - \mu_{k(\mathbf{x})}) \cdot z_{k(\mathbf{x})}(\mathbf{x})\big)\Big)\Big\} \end{aligned} \tag{2}$$

Here, the function $\xi_\gamma : \mathbb{R} \to \mathbb{R}^+$ is given by:

$$\xi_\gamma(w) = \frac{w^2}{2\gamma} \cdot \mathbb{I}\{0 \leq w \leq \gamma\} \;+\; \big(w - \frac{\gamma}{2}\big) \cdot \mathbb{I}\{w > \gamma\} \tag{3}$$

Note that ξ_γ is convex and its derivative ξ'_γ is $(1/\gamma)$-Lipschitz continuous, and it can be interpreted as differentiable approximation to the ReLU unit (Nair and Hinton, 2010). A full pseudocode of the proposed algorithm is presented in Appendix A.

4 Theoretical Analysis

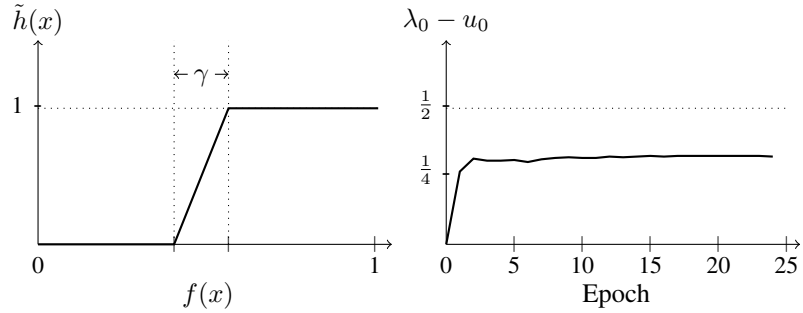
We will first show (Appendix B) that attaining conditional statistical parity as specified in Definition 1 is, generally, *impossible* unless the groups are known in advance.

Proposition 1 (Impossibility result)**.** *Let $\mathcal{X}$ be the instance space and $\mathcal{Y} = \{0,\, 1\}$ be a target set. Let $1_S : \mathcal{X} \to \{0, 1\}$ be an arbitrary (possibly randomized) binary-valued function on $\mathcal{X}$ and define $\gamma : \mathcal{X} \to [0, 1]$ by $\gamma(x) = p(1_S(\boldsymbol{x}) = 1 \,|\, \boldsymbol{x} = x)$, where the probability is evaluated over the randomness of $1_S : \mathcal{X} \to \{0, 1\}$. Write $\bar{\gamma} = \mathbb{E}_{\boldsymbol{x}}[\gamma(\boldsymbol{x})]$. Then, for any binary predictor $f : \mathcal{X} \to \{0, 1\}$ it holds that*

$$\sup_{\pi:\, \mathcal{X} \to \{0,1\}} \Big\{\mathbb{E}_{\pi(\boldsymbol{x})} \big|\mathcal{C}\big(f(\boldsymbol{x}), \gamma(\boldsymbol{x}) |\, \pi(\boldsymbol{x})\big)\big|\Big\} \geq \; \frac{1}{2}\, \mathbb{E}_{\boldsymbol{x}} |\gamma(\boldsymbol{x}) - \bar{\gamma}| \cdot \min\{\mathbb{E} f, 1 - \mathbb{E} f\}, \tag{4}$$

where $\mathcal{C}\big(f(\boldsymbol{x}), \gamma(\boldsymbol{x}) |\, \pi(\boldsymbol{x})\big)$ is defined in Definition 1.

[1] Ideally an estimate of some monotone transformation of $2\eta(x) - 1$, where $\eta(x) = p(\mathbf{y} = 1 | \mathbf{x} = x)$ is the Bayes regressor. This is not a strong assumption because many algorithms can be calibrated to provide probability scores (Platt et al., 1999; Guo et al., 2017).



(a) Decision rule (b) Convergence

Figure 2: (a) The learned post-processing decision rule $\tilde{h}(x)$ in Equation 1 as a function of the classifier's score $f(x)$. Randomization is applied when $\tilde{h}(x) \in (0, 1)$, which can be controlled using the regularization parameter $\gamma > 0$. (b) The value of $\lambda_0 - u_0$ is plotted against the number of epochs in the projected SGD method applied to the output of the random forests classifier trained on the Adult dataset to implement statistical parity with respect to the gender attribute (cf. Section 5 and Figure 1). We observe fast convergence in agreement with Proposition 2.

Consequently, a deterministic classifier $f : \mathcal{X} \to \{0, 1\}$ cannot be universally unbiased with respect to a sensitive class S across all possible known and unknown groups unless the representation $\mathbf{x}$ has zero mutual information with the sensitive attribute or if f is constant almost everywhere. As a corollary, the groups X_k have to be known *in advance*.

Next, we show that the prediction rule in Equation 1 learned through the update rules presented in Section 3 enjoy the desired fairness guarantees.

Theorem 1 (Correctness)**.** *Let $\tilde{h}_\gamma : \mathcal{X} \to \{0, 1\}$ be the randomized predictor defined in Equation 1 learned by applying the update rules in Equation 2 starting with $\mu_k = 0, \lambda_k = 0, \forall k \in [K]$ until convergence. Then, $\tilde{h}_\gamma$ satisfies ϵ conditional statistical parity w.r.t. the groups $\{X_k\}_{k\in[K]}$.*

The proof of Theorem 1 is presented in Appendix C. Our next theorem shows that the randomized prediction rule converges to the Bayes optimal unbiased classifier if the original classifier f is Bayes consistent. The proof of the following theorem (Appendix D) is based on the Lipschitz continuity of the decision rule when $\gamma > 0$ and the robustness framework of Xu and Mannor (2012).

Theorem 2. *Let $h^\star = \arg\min_{h\in\mathcal{H}} \mathbb{E}[h(\boldsymbol{x}) \neq \mathbf{y}]$, where $\mathcal{H}$ is the set of binary predictors on $\mathcal{X}$ that satisfy fairness according to Definition 1 for some $\epsilon > 0$. Let $\tilde{h}_\gamma : \mathcal{X} \to \{0, 1\}$ be the randomized learning rule in Equation 1. If $\tilde{h}_\gamma$ is trained on a freshly sampled data of size N, then with a probability of at least $1 - \delta$:*

$$\mathbb{E}[\tilde{h}_\gamma(\boldsymbol{x}) \neq \mathbf{y}] \leq \mathbb{E}[h^\star(\boldsymbol{x}) \neq \mathbf{y}] + \mathbb{E}\left|2\eta(\boldsymbol{x}) - 1 - f(\boldsymbol{x})\right| + 2\gamma + \frac{8(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 4\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}},$$

where $\eta : \mathcal{X} \to [0, 1]$ is the Bayes regressor.

Consequently, if the original classifier is Bayes consistent and we have: $N \to \infty$, $\gamma \to 0^+$ and $\gamma N^{-\frac{1}{3}} \to \infty$, then $\mathbb{E}[\tilde{h}_\gamma(\mathbf{x}) \neq \mathbf{y}] \xrightarrow{P} \mathbb{E}[h^\star(\mathbf{x}) \neq \mathbf{y}]$. Hence, the updates converge to the *optimal* prediction rule subject to the chosen fairness constraint.

Running time As shown in Appendix C, the update rules in Equation 2 perform a projected stochastic gradient descent on the following optimization problem:

$$\min_{(\mu_1,\lambda_1),\ldots,(\mu_K,\lambda_K)\geq 0} F = \mathbb{E}_{\mathbf{x}}\Big[\epsilon(\lambda_{k(\mathbf{x})} + \mu_{k(\mathbf{x})}) + \xi_\gamma(f(\mathbf{x}) - (\lambda_{k(\mathbf{x})} - \mu_{k(\mathbf{x})})z_{k(\mathbf{x})}(\mathbf{x}))\Big] \quad (5)$$

We assume with no loss of generality that $f(x) \in [-1, 1]$ since $f(x)$ is assumed to be an estimator to $2\eta(x) - 1$ (see Section 3 and Appendix C) and any thresholding rule over $f(x)$ can be transformed into an equivalent rule over a monotone increasing function of f (i.e. using the hyperbolic tangent).

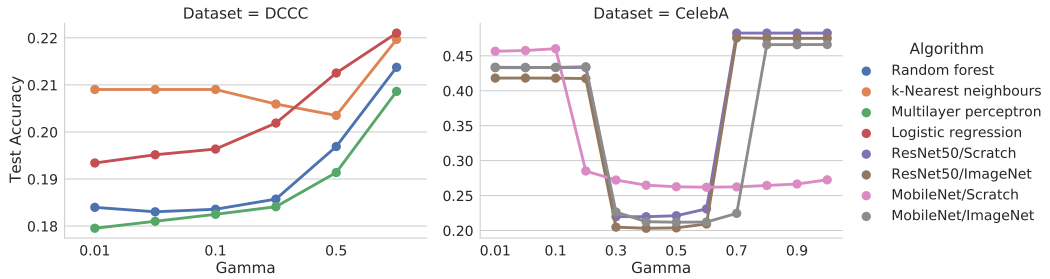


Figure 3: A plot of the test accuracy vs. the parameter γ for both the DCCC and CelebA datasets. The curves correspond to different original classifiers. In general, having a small value $\gamma \ll 1$ yields better results but for some classifiers, such as k-NN or neural networks, in which randomization at the threshold is often necessary, it is best to tune the value of γ with a validation dataset.

Proposition 2. *Let $\mu^{(0)} = \lambda^{(0)} = 0$ and write $\mu^{(t)}, \lambda^{(t)} \in \mathbb{R}^K$ for the value of the optimization variables after t updates defined in Equation 2 for some fixed learning rate $\alpha_t = \alpha$. Let $\bar{\mu} = (1/T)\sum_{t=1}^{T} \mu^{(t)}(x)$ and $\bar{\lambda} = (1/T)\sum_{t=1}^{T} \lambda^{(t)}(x)$. Then,*

$$\mathbb{E}[\bar{F}] - F(\mu^\star)\big) \leq \frac{(1+\epsilon+b)^2\alpha}{2} + \frac{||\mu^\star||_2^2 + ||\gamma^\star||_2^2}{2T\alpha}, \tag{6}$$

where $\bar{F} : \mathbb{R}^K \times \mathbb{R}^K \to \mathbb{R}$ is the objective function in (5) using the averaged solution $\bar{\mu}$ and $\bar{\lambda}$ while $F^\star$ is its optimal value. In particular, $\mathbb{E}[\bar{F}] - F(\mu^\star)\big) = \mathcal{O}(\sqrt{K/T})$ when $\alpha = \mathcal{O}(\sqrt{K/T})$.

The proof is in Appendix E. Hence, the post-processing rule can be efficiently computed. In practice, we observe fast convergence as shown in Figure 2(b).

As shown in Figure 2(a), the hyperparameter γ controls the width of randomization around the thresholds. A large value of γ may reduce the accuracy of the classifier. On the other hand, γ cannot be zero because randomization around the threshold is, in general, necessary for Bayes risk consistency as illustrated in the following example:

Example 1 (Randomization is necessary)**.** *Suppose that $\mathcal{X} = \{-1, 0, 1\}$ where $p(\boldsymbol{x} = -1) = 1/2$, $p(\boldsymbol{x} = 0) = 1/3$ and $p(\boldsymbol{x} = 1) = 1/6$. Let $\eta(-1) = 0$, $\eta(0) = 1/2$ and $\eta(1) = 1$. In addition, let $\boldsymbol{s}$ be a sensitive attribute, where $p(\boldsymbol{s} = 1|\boldsymbol{x} = -1) = 1/2$, $p(\boldsymbol{s} = 1|\boldsymbol{x} = 0) = 1$, and $p(\boldsymbol{s} = 1|\boldsymbol{x} = 1) = 0$. Then, the Bayes optimal prediction rule $f^\star$ subject to statistical parity w.r.t. $\boldsymbol{s}$ satisfies: $p(f^\star = 1|\boldsymbol{x} = -1) = 0$, $p(f^\star = 1|\boldsymbol{x} = 0) = 1/2$ and $p(f^\star = 1|\boldsymbol{x} = 1) = 1$.*

Note that the Bayes excess risk bound in Theorem 2 is vacuous when $\gamma = 0$. Therefore, γ controls a trade-off depending on how crucial randomization is around the thresholds (e.g. in k-NN where the classifier's scores come from a finite set) which is demonstrated in Figure 3. In our experiments, γ is always chosen using a validation set.

5 Empirical Evaluation

Tabular Data We empirically evaluate the performance of the proposed algorithm and the baselines on two real-world datasets, namely the Adult income dataset and the Default of Credit Card Clients (DCCC) dataset, both taken from the UCI Machine Learning Repository (Blake and Merz, 1998). The Adult dataset contains 48,842 records with 14 attributes each and the goal is to predict if the income of an individual exceeds \$50K per year. The DCCC dataset contains 30,000 records with 24 attributes, and the goal is to predict if a client will default on their credit card payment. Both datasets include sensitive attributes, such as sex and age. In Figure 1 we showcased why *conditional* statistical parity is critical to ensure that females and males are treated equally across all demographic groups. However, since the demographic groups are disjoint, it suffices to focus on (unconditional) statistical parity to fairly compare the proposed algorithm to the existing baselines. In our experiments, we define the sensitive class S to be the class of females. In the DCCC dataset, we additionally introduce bias in the training set for the purpose of the experiment: if $1_S(\mathbf{x}) = y(\mathbf{x})$ we keep the instance and otherwise drop it with probability 0.5.

Bias					
Dataset	Classifier	Original	Proposed	Hardt et al. (2016)	Shift Inference
ADULT	RF	.026±.002	.003±.001	.003±.001	.025±.002
	kNN	.030±.001	.004±.001	.002±.001	.018±.002
	MLP	.028±.001	.003±.001	.004±.001	.023±.001
	LR	.030±.001	.001±.001	.002±.001	.017±.002
CDDD	RF	.051±.001	.009±.001	.003±.001	.005±.002
	kNN	.058±.001	.004±.001	.002±.001	.007±.002
	MLP	.060±.001	.004±.002	.001±.001	.012±.001
	LR	.063±.001	.003±.001	.001±.001	.005±.001

Test error					
Dataset	Classifier	Original	Proposed	Hardt et al. (2016)	Shift Inference
ADULT	RF	34.0±.1%	35.6±.2%	37.7±.1%	35.0±.1%
	kNN	39.6±.1%	39.7±.2%	41.8±.1%	39.2±.2%
	MLP	34.4±.1%	36.3±.1%	37.4±.2%	35.7±.1%
	LR	35.2±.1%	36.5±.2%	39.1±.1%	35.9±.1%
CDDD	RF	18.81±.2%	18.4±.1%	20.7±.1%	18.2±.1%
	kNN	20.7±.2%	20.3±.2%	21.4±.1%	19.5±.2%
	MLP	19.6±.1%	18.3±.2%	20.9±.2%	18.5±.1%
	LR	19.9±.2%	19.2±.1%	21.9±.1%	18.8±.2%

Table 1: A comparison of the three post-processing methods on two datasets with four different original classifiers. Both the proposed algorithm and the algorithm of Hardt et al. (2016) eliminate bias in all cases whereas Shift Inference is not guaranteed to eliminate bias. Bias here is the absolute value of the covariance between the sensitive attribute and the classifier's predictions. On the other hand, the proposed algorithm significantly outperforms Hardt et al. (2016) in terms of test accuracy.

We train four classifiers on each dataset: (1) random forests with maximum depth 10, (2) k-NN with $k = 10$, (3) a two-layer fully connected neural network with 128 hidden nodes, and (4) logistic regression. For the latter, we fine-tune the parameter C in a grid of values chosen in a logarithmic scale between 10^{-4} and 10^4 using 10-fold cross validation. The learning rate in our algorithm is fixed to $10^{-1}(K/T)^{1/2}$, where T is the number of steps, and $\epsilon = 0$.

We compare against two standard post-processing methods: (1) the post-processing algorithm of Hardt et al. (2016) and (2) the shift inference method, first introduced in (Saerens et al., 2002) and used more recently in (Royer and Lampert, 2015; Wang et al., 2020). We use the implementation of the algorithm of Hardt et al. (2016) in the FairLearn software package (Dudik et al., 2020).

Table 1 shows the bias and accuracy on *test* data after applying each post-processing method. The first column, marked as "original", corresponds to the original classifier without any alteration. As shown in the table, both our proposed post-processing algorithm and the algorithm of Hardt et al. (2016) eliminate bias in all classifiers. By contrast, the shift-inference method does not always eliminate bias. However, the proposed algorithm has a much lower impact on the test accuracy and can even improve it in certain cases. The fact that fairness can sometimes improve the test accuracy was recently noted by Blum and Stangl (2020).

CelebA Dataset Our second set of experiments builds on the task of predicting the "attractiveness" attribute in the CelebA dataset (Liu et al., 2015). CelebA contains 202,599 images of celebrities annotated with 40 binary attributes, such as gender, attractiveness, and smiling. We use two standard deep neural network architectures: ResNet50 (He et al., 2016) and MobileNet Howard et al. (2017), either trained from scratch or pretrained on ImageNet. We present the results in Table 2.

We observe that the proposed algorithm outperforms others significantly in terms of both bias and test accuracy. We investigated this strong performance and found that it is due to the specific form of randomization used by the proposed algorithm. As shown in Figure 4, the post-processing algorithm of Hardt et al. (2016) uses a fixed probability when randomizing between two thresholds. For

Bias					
Model	Training	Original	Proposed	Hardt et al. (2016)	Shift Inference
RESNET50	SCRATCH	.12	.004	.02	.04
	IMAGENET	.11	.001	.02	.06
MOBILENET	SCRATCH	.10	.008	.02	.002
	IMAGENET	.10	.004	.01	.05

Test error					
Model	Training	Original	Proposed	Hardt et al. (2016)	Shift Inference
RESNET50	SCRATCH	21.5%	23.3%	34.3%	39.4%
	IMAGENET	19.5%	20.8%	31.4%	31.6%
MOBILENET	SCRATCH	22.8%	26.9%	33.7%	49.3%
	IMAGENET	20.5%	22.5%	33.0%	36.4%

Table 2: A comparison of the three post-processing methods on CelebA (predict attractiveness) applied to the output of ResNet50 and MobileNet, each trained either from scratch or on ImageNet.

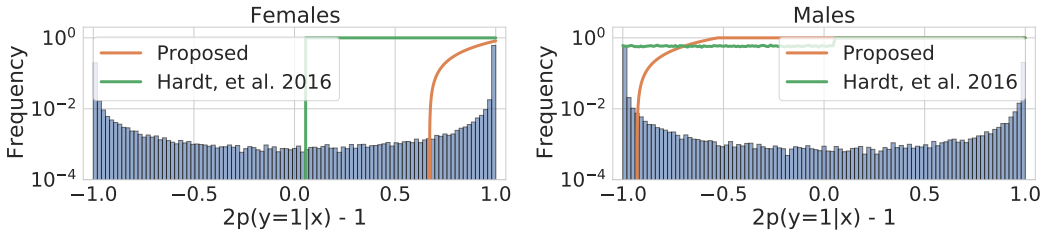


Figure 4: The distribution of the scores produced by ResNet50 trained from scratch are shown for both subpopulations. The curves correspond to the post-processing rules, i.e. $p(\mathbf{y} = 1|\mathbf{x})$, of the proposed algorithm and Hardt et al. (2016).

CelebA trained from scratch, for example, the post-processing rule of Hardt et al. (2016) predicts nearly uniformly at random when ResNet50 predicts the negative class for males. In contrast, our algorithm uses a ramp function that takes the confidence of the scores into account so that most of the instances whose labels are altered by the post-processing rule are close to the decision boundary of the original classifier. The best accuracy of the proposed algorithm is achieved with $\gamma = 0.4$ (Figure 3). We remark that the value of γ is always chosen on a separate validation dataset.

Lastly, one important observation we note in Table 2 is the impact of *pre-training* – pretraining helps in achieving a lower test error rate even after eliminating bias. In other words, pretraining reduces the cost of debiasing trained models.

6 CONCLUDING REMARKS

In this paper, we propose a near-optimal post-processing algorithm for debiasing trained machine learning models. The proposed algorithm is scalable, does not require retraining the classifiers, and has a limited impact on the test accuracy. In addition to providing strong theoretical guarantees, we show that it outperforms previous post-processing methods for unbiased classification on standard benchmarks across classical and modern machine learning models.

REFERENCES

M. A. Bruckner, "The promise and perils of algorithmic lenders' use of big data," *Chi.-Kent L. Rev.*, 2018.

R. C. Deo, "Machine learning in medicine," *Circulation*, 2015.

T. Brennan, W. Dieterich, and B. Ehret, "Evaluating the predictive validity of the COMPAS risk and needs assessment system," *Criminal Justice and Behavior*, 2009.

E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J.-F. Bonnefon, and I. Rahwan, "The moral machine experiment," *Nature*, 2018.

J. Kleinberg, S. Mullainathan, and M. Raghavan, "Inherent trade-offs in the fair determination of risk scores," 2017.

D. Ingold and S. Soper, "Amazon doesnt consider the race of its customers. should it," *Bloomberg News*, 2016.

C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness through awareness," in *Innovations in Theoretical Computer Science*, 2012.

M. B. Zafar, I. Valera, M. Gomez Rodriguez, and K. P. Gummadi, "Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment," in *International Conference on World Wide Web*, 2017.

M. Hardt, E. Price, N. Srebro *et al.*, "Equality of opportunity in supervised learning," in *Advances in Neural Information Processing Systems*, 2016.

A. Chouldechova, "Fair prediction with disparate impact: A study of bias in recidivism prediction instruments," *Big data*, 2017.

L. Dixon, J. Li, J. Sorensen, N. Thain, and L. Vasserman, "Measuring and mitigating unintended bias in text classification," in *Conference on AI, Ethics, and Society*, 2018.

S. Corbett-Davies, E. Pierson, A. Feller, S. Goel, and A. Huq, "Algorithmic decision making and the cost of fairness," in *International Conference on Knowledge Discovery and Data Mining*, 2017.

N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," *arXiv preprint arXiv:1908.09635*, 2019.

C. L. Blake and C. J. Merz, "UCI repository of machine learning databases," Irvine, CA, 1998.

M. B. Zafar, I. Valera, M. Gomez-Rodriguez, and K. P. Gummadi, "Fairness Constraints: A Flexible Approach for Fair Classification," *Journal of Machine Learning Research*, 2019.

R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork, "Learning fair representations," in *International Conference on Machine Learning*, 2013.

K. Lum and J. Johndrow, "A statistical framework for fair predictive algorithms," *arXiv preprint arXiv:1610.08077*, 2016.

T. Bolukbasi, K.-W. Chang, J. Y. Zou, V. Saligrama, and A. T. Kalai, "Man is to computer programmer as woman is to homemaker? debiasing word embeddings," in *Advances in Neural Information Processing Systems*, 2016.

F. Calmon, D. Wei, B. Vinzamuri, K. N. Ramamurthy, and K. R. Varshney, "Optimized preprocessing for discrimination prevention," in *Advances in Neural Information Processing Systems*, 2017.

D. Madras, E. Creager, T. Pitassi, and R. Zemel, "Learning adversarially fair and transferable representations," in *International Conference on Machine Learning*, 2018.

F. Kamiran and T. Calders, "Data preprocessing techniques for classification without discrimination," *Knowledge and Information Systems*, 2012.

——, "Classifying without discriminating," in *International Conference on Computer, Control and Communication*, 2009.

F. Locatello, G. Abbati, T. Rainforth, S. Bauer, B. Schölkopf, and O. Bachem, "On the fairness of disentangled representations," in *Advances in Neural Information Processing Systems*, 2019.

B. H. Zhang, B. Lemoine, and M. Mitchell, "Mitigating unwanted biases with adversarial learning," in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018.

N. Grgić-Hlača, M. B. Zafar, K. P. Gummadi, and A. Weller, "Beyond distributive fairness in algorithmic decision making: Feature selection for procedurally fair learning," in *AAAI Conference on Artificial Intelligence*, 2018.

A. Agarwal, A. Beygelzimer, M. Dudik, J. Langford, and H. Wallach, "A reductions approach to fair classification," in *International Conference on Machine Learning*, 2018.

A. K. Menon and R. C. Williamson, "The cost of fairness in binary classification," in *Conference on Fairness, Accountability and Transparency*, 2018.

L. E. Celis, L. Huang, V. Keswani, and N. K. Vishnoi, "Classification with fairness constraints: A meta-algorithm with provable guarantees," in *Conference on Fairness, Accountability, and Transparency*, 2019.

B. Fish, J. Kun, and Á. D. Lelkes, "A confidence-based approach for balancing fairness and accuracy," in *International Conference on Data Mining*, 2016.

B. Woodworth, S. Gunasekar, M. I. Ohannessian, and N. Srebro, "Learning non-discriminatory predictors," *arXiv preprint arXiv:1702.06081*, 2017.

L. Bottou, "Large-scale machine learning with stochastic gradient descent," in *International Conference on Computational Statistics*, 2010.

M. B. Zafar, I. Valera, M. G. Rogriguez, and K. P. Gummadi, "Fairness Constraints: Mechanisms for Fair Classification," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 2017.

J. Platt *et al.*, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," *Advances in Large Margin Classifiers*, 1999.

C. Guo, G. Pleiss, Y. Sun, and K. Q. Weinberger, "On calibration of modern neural networks," in *International Conference on Machine Learning*, 2017.

V. Nair and G. E. Hinton, "Rectified linear units improve restricted boltzmann machines," in *International Conference on Machine Learning*, 2010.

H. Xu and S. Mannor, "Robustness and generalization," *Machine learning*, 2012.

M. Saerens, P. Latinne, and C. Decaestecker, "Adjusting the outputs of a classifier to new a priori probabilities: a simple procedure," *Neural Computation*, 2002.

A. Royer and C. H. Lampert, "Classifier adaptation at prediction time," in *Conference on Computer Vision and Pattern Recognition*, 2015.

Z. Wang, K. Qinami, I. C. Karakozis, K. Genova, P. Nair, K. Hata, and O. Russakovsky, "Towards fairness in visual recognition: Effective strategies for bias mitigation," in *Conference on Computer Vision and Pattern Recognition*, 2020.

M. Dudik, R. Edgar, B. Horn, and R. Lutz, "fairlearn 0.4.6," 2020. [Online]. Available: https://pypi.org/project/fairlearn/

A. Blum and K. Stangl, "Recovering from biased data: Can fairness constraints improve accuracy?" *FROC*, 2020.

Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *International Conference on Computer Vision*, 2015.

K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Conference on Computer Vision and Pattern Recognition*, 2016.

A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," *arXiv preprint arXiv:1704.04861*, 2017.

S. Boyd and A. Mutapcic, "Stochastic subgradient methods," 2008. [Online]. Available: https://see.stanford.edu/materials/lsocoee364b/04-stoch_subgrad_notes.pdf

S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.

A FULL ALGORITHM

Algorithm 2: A Pseudocode of the Proposed Algorithm for Conditional Statistical Parity.

Data: $\gamma > 0;\ \epsilon \geq 0;\ f : \mathcal{X} \to [-1, +1]; k : \mathcal{X} \to [K]$

Result: Optimal values of thresholds: $(\lambda_1, \mu_1), \ldots, (\lambda_K, \mu_K)$.

Training: Initialize $(\lambda_1, \mu_1), \ldots, (\lambda_K, \mu_K)$ to zeros. Then, repeat until convergence:

1. Sample an instance $\mathbf{x} \sim p(x)$
2. Perform the updates:

$$\lambda_{k(\mathbf{x})} \leftarrow \max\Big\{0,\ \lambda_{k(\mathbf{x})} - \eta\Big(\epsilon + \frac{\partial}{\partial \lambda_{k(\mathbf{x})}} \xi_\gamma\big(f(\mathbf{x}) - (\lambda_{k(\mathbf{x})} - \mu_{k(\mathbf{x})}) \cdot z_{k(\mathbf{x})}(\mathbf{x})\big)\Big)\Big\}$$

$$\mu_{k(\mathbf{x})} \leftarrow \max\Big\{0,\ \mu_{k(\mathbf{x})} - \eta\Big(\epsilon + \frac{\partial}{\partial \mu_{k(\mathbf{x})}} \xi_\gamma\big(f(\mathbf{x}) - (\lambda_{k(\mathbf{x})} - \mu_{k(\mathbf{x})}) \cdot z_{k(\mathbf{x})}(\mathbf{x})\big)\Big)\Big\},$$

where ξ_γ is given by Eq. (3), $z_k(x) = 1_S(x) - \rho_k$, and $\rho_k = \mathbb{E}_{\mathbf{x}}[1_S(\mathbf{x}) \,|\, \mathbf{x} \in X_k]$.

Prediction: Given an instance x in the group X_k, predict the label $+1$ with probability:

$$\tilde{h}(x) = \begin{cases} 0, & f(x) \leq (\lambda_k - \mu_k) z(x) \\ (f(x) - (\lambda_k - \mu_k) z(x))/\gamma, & (\lambda_k - \mu_k) z(x) \leq f(x) \leq (\lambda_k - \mu_k) z(x) + \gamma \\ 1, & f(x) \geq (\lambda_k - \mu_k) z(x) + \gamma \end{cases}$$

B PROOF OF PROPOSITION 1

Proof. Fix $0 < \beta < 1$ and consider the subset:

$$W = \{x \in \mathcal{X} :\ (\gamma(x) - \bar{\gamma}) \cdot (f(x) - \beta) > 0\},$$

and its complement $\bar{W} = \mathcal{X} \setminus W$. Since $f(x) \in \{0, 1\}$, the sets W and $\bar{W}$ are independent of β as long as it remains in the open interval $(0,\ 1)$. More precisely:

$$W = \begin{cases} \gamma(x) - \bar{\gamma} > 0 & \wedge \quad f(x) = 1 \\ \gamma(x) - \bar{\gamma} \leq 0 & \wedge \quad f(x) = 0 \end{cases}$$

Now, for any set $X \subseteq \mathcal{X}$, let p_X be the projection of the probability measure $p(x)$ on the set X (i.e. $p_X(x) = p(x)/p(X)$). Then, with a simple algebraic manipulation, one has the identity:

$$\mathbb{E}_{\mathbf{x}\sim p_X}\left[(\gamma(\mathbf{x}) - \bar{\gamma})\,(f(\mathbf{x}) - \beta)\right] = C(\gamma(\mathbf{x}), f(\mathbf{x}); \mathbf{x} \in X) + (\mathbb{E}_{\mathbf{x}\sim p_X}[\gamma] - \bar{\gamma}) \cdot (\mathbb{E}_{\mathbf{x}\sim p_X}[f] - \beta) \quad (7)$$

By definition of W, we have:

$$\mathbb{E}_{\mathbf{x}\sim p_W}[(\gamma(\mathbf{x}) - \bar{\gamma})(f(\mathbf{x}) - \beta)] = \mathbb{E}_{\mathbf{x}\sim p_W}[|\gamma(\mathbf{x}) - \bar{\gamma}||f(\mathbf{x}) - \beta|] \geq \min\{\beta, 1 - \beta\}\mathbb{E}_{\mathbf{x}\sim p_W}|\gamma(\mathbf{x}) - \bar{\gamma}|$$

Combining this with Eq. (7), we have:

$$C(\gamma(\mathbf{x}), f(\mathbf{x}); \mathbf{x} \in W) \geq \min\{\beta, 1 - \beta\}\mathbb{E}_{\mathbf{x}\sim p_W}|\gamma(\mathbf{x}) - \bar{\gamma}| + (\mathbb{E}_{\mathbf{x}\sim p_W}[\gamma] - \bar{\gamma})(\beta - \mathbb{E}_{\mathbf{x}\sim p_W}[f]) \quad (8)$$

Since the set W does not change when β is varied in the open interval $(0,\ 1)$, the lower bound holds for any value of $\beta \in (0, 1)$. W set:

$$\beta = \bar{f} \doteq \frac{1}{2}\big(\mathbb{E}_{\mathbf{x}\sim p_W} f(\mathbf{x}) \ +\ \mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}} f(\mathbf{x})\big) \quad (9)$$

Substituting the last equation into Eq. (8) gives the lower bound:

$$\begin{aligned} C(\gamma(\mathbf{x}), f(\mathbf{x}); \mathbf{x} \in W) \geq & \min\{\bar{f}, 1 - \bar{f}\} \cdot \mathbb{E}_{\mathbf{x}\sim p_W}|\gamma(\mathbf{x}) - \bar{\gamma}| \\ & + \frac{1}{2}(\mathbb{E}_{\mathbf{x}\sim p_W}[\gamma] - \bar{\gamma})\,\big(\mathbb{E}_{\mathbf{x}\sim p_W} f(\mathbf{x}) - \mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}} f(\mathbf{x})\big) \end{aligned} \quad (10)$$

Repeating the same analysis for the subset $\bar{W}$, we arrive at the inequality:

$$C(\gamma(\mathbf{x}), f(\mathbf{x}); \mathbf{x} \in \bar{W}) \leq -\min\{\bar{f}, 1-\bar{f}\}\, \mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}} |\gamma(\mathbf{x}) - \bar{\gamma}| + \frac{1}{2}(\mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}}[\gamma] - \bar{\gamma}) \left(\mathbb{E}_{\mathbf{x}\sim p_W} f(\mathbf{x}) - \mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}} f(\mathbf{x})\right) \tag{11}$$

Writing $\pi(x) = 1_W(x)$, we have by the reverse triangle inequality:

$$\mathbb{E}_{\pi(\mathbf{x})} \left|\mathcal{C}\big(f(\mathbf{x}), \gamma(\mathbf{x});\ \pi(\mathbf{x})\big)\right| \geq \min\{\bar{f}, 1-\bar{f}\} \cdot \mathbb{E}_{\mathbf{x}} |\gamma(\mathbf{x}) - \bar{\gamma}| \tag{12}$$

Finally:

$$2\bar{f} \geq p(\mathbf{x} \in W) \cdot \mathbb{E}_{\mathbf{x}\sim p_W} f(\mathbf{x}) \ + \ p(\mathbf{x} \in \bar{W}) \cdot \mathbb{E}_{\mathbf{x}\sim p_{\bar{W}}} f(\mathbf{x}) = \mathbb{E}[f]$$

Similarly, we have $2(1-\bar{f}) \geq 1 - \mathbb{E}[f]$. Therefore:

$$\min\{\bar{f},\, 1-\bar{f}\} \geq \frac{1}{2}\, \min\{\mathbb{E}f,\, 1-\mathbb{E}f\}$$

Combining this with Eq. (12) establishes the statement of the proposition. □

C Proof of Theorem 1

C.1 Constrained Convex Formulation

Suppose we have a binary classifier on the instance space $\mathcal{X}$. We would like to construct an algorithm for post-processing the predictions made by that classifier such that we control the bias with respect to a sensitive attribute $1_S : \mathcal{X} \to \{0, 1\}$ across a fixed set of pairwise disjoint groups $X_1, \ldots, X_K \subseteq \mathcal{X}$. We assume that the output of the classifier $f : \mathcal{X} \to [-1, +1]$ is an estimate to $2\eta(x) - 1$, where $\eta(x) = p(\mathbf{y} = 1|\mathbf{x} = x)$ is the Bayes regressor. This is not a strong assumption because many algorithms can be calibrated to provide probability scores (Platt et al., 1999; Guo et al., 2017) so the assumption is valid. We consider randomized rules of the form:

$$\tilde{f} : \mathcal{X} \times \{1, 2, \ldots, K\} \times \{0, 1\} \times [-1,\, 1] \to \{0, 1\},$$

whose arguments are: (1) the instance $\mathbf{x} \in \mathcal{X}$, (2) the group X_k, (3) the sensitive attribute $1_S(x)$, and (4) the original classifier's score $f(x)$. Because randomization is sometimes necessary as proved in Section 4, $\tilde{f}(x)$ is the probability of predicting the positive class when the instance is $x \in \mathcal{X}$.

Suppose we have a training sample of size N, which we will denote by $\mathcal{S}$. Let $q_i = \tilde{f}(x_i) \in [0,\, 1]$ for the i-th instance in $\mathcal{S}$. For each group $X_k \subseteq \mathcal{S}$, the fairness constraint in Definition 1 can be written as:

$$\frac{1}{|X_k|} \Big| \sum_{i \in X_k} (1_S(i) - \rho_k)\, q_i \Big| \ \leq \ \epsilon_0$$

This is because:

$$\begin{aligned}
\frac{1}{|X_k|} \sum_{i \in X_k} (1_S(i) - \rho_k)\, q_i &= \frac{1}{|X_k|} \sum_{i \in X_k} 1_S(i)\, \tilde{f}(i) - \frac{\rho_k}{|X_k|} \sum_{i \in X_k} \tilde{f}(i) \\
&= \mathbb{E}[1_S(\mathbf{x}) \cdot \tilde{f}(\mathbf{x}) \,|\, \mathbf{x} \in X_k] - \mathbb{E}[1_S(\mathbf{x}) | \,\mathbf{x} \in X_k] \cdot \mathbb{E}[\tilde{f}(\mathbf{x}) \,|\, \mathbf{x} \in X_k] \\
&= C(\tilde{f}(\mathbf{x}),\, 1_S(\mathbf{x}) \,|\, \mathbf{x} \in X_k)
\end{aligned}$$

To learn $\tilde{f}$, we propose solving the following *regularized* optimization problem:

$$\min_{0 \leq q_i \leq 1} \quad \sum_{i=1}^{N} (\gamma/2)\, q_i^2 \ - \ f(x_i)\, q_i \quad \text{s.t.} \quad \forall X_k \in \mathcal{G} : \Big| \sum_{i \in X_k} (1_S(i) - \rho_k)\, q_i \Big| \ \leq \ \epsilon_k \tag{13}$$

where $\gamma \ll 1$ is a regularization parameter and $\epsilon_k = |X_k|\, \epsilon_0$. To gain an intuition for this, note that if $\gamma = 0$, then minimizing the objective function alone is equivalent to the thresholding rule $q_i = \mathbb{I}\{f(i) \geq 0\}$, which is the Bayes optimal rule if $f(i) = 2\eta(i) - 1$.

C.2 Reduction to Unconstrained Optimization

Because the groups X_k are pairwise disjoint, the optimization problems in (13) decomposes into K separate suboptimization problems, one for each group X_k. Each sub-optimization problem can be written in the following general form:

$$\begin{aligned} \min_{0 \le q_i \le 1} \quad & \sum_{i=1}^{M} \frac{\gamma}{2} q_i^2 - f(x_i) q_i \\ \text{s.t.} \quad & \sum_{i=1}^{M} (z_i q_i - b) \le \epsilon, \qquad -\sum_{i=1}^{M} (z_i q_i - b) \le \epsilon \end{aligned}$$

To recall, $\epsilon = M\epsilon_0$. The Lagrangian is:

$$L(q, \alpha, \beta, \lambda, \mu) =$$
$$\sum_i \big(\frac{\gamma}{2} q_i^2 - f(x_i) q_i\big) + \lambda(\sum_i (z_i q_i - b) - \epsilon) - \mu(\sum_i (z_i q_i - b) + \epsilon) + \sum_i \alpha_i (q_i - 1) - \sum_i \beta_i q_i$$

Taking the derivative w.r.t. q_i gives us:

$$q_i = \frac{1}{\gamma}\Big(f(x_i) - (\lambda - \mu) z_i - \alpha_i + \beta_i\Big)$$

Plugging this back, the dual problem becomes:

$$\begin{aligned} \min_{q, \lambda, \mu, \alpha, \beta} \quad & \sum_i \big(\frac{\gamma}{2} q_i^2 + b(\lambda - \mu)\big) + (\lambda + \mu)\epsilon + \sum_i \alpha_i \\ \text{s.t.} \quad & q_i = \frac{1}{\gamma}\Big(f(x_i) - (\lambda - \mu) z_i - \alpha_i + \beta_i\Big) \\ & \lambda, \mu, \alpha_i, \beta_i \ge 0 \end{aligned}$$

Next, we eliminate variables. By eliminating β_i, we have:

$$\begin{aligned} \min_{q, \lambda, \mu, \alpha, \beta} \quad & \sum_i \big(\frac{\gamma}{2} q_i^2 + b(\lambda - \mu)\big) + (\lambda + \mu)\epsilon + \sum_i \alpha_i \\ \text{s.t.} \quad & q_i - \frac{1}{\gamma}\Big(f(x_i) - (\lambda - \mu) z_i - \alpha_i\Big) \ge 0 \\ & \lambda, \mu, \alpha_i \ge 0 \end{aligned}$$

Equivalently:

$$\begin{aligned} \min_{q, \lambda, \mu, \alpha, \beta} \quad & \sum_i \big(\frac{\gamma}{2} q_i^2 + b(\lambda - \mu)\big) + (\lambda + \mu)\epsilon + \sum_i \alpha_i \\ \text{s.t.} \quad & \alpha_i \ge f(x_i) - \gamma q_i - (\lambda - \mu) z_i \\ & \lambda, \mu, \alpha_i \ge 0 \end{aligned}$$

Next, we eliminate α_i to obtain:

$$\begin{aligned} \min_{q, \lambda, \mu} \quad & \sum_i \big(\frac{\gamma}{2} q_i^2 + b(\lambda - \mu)\big) + (\lambda + \mu)\epsilon + \sum_i \big[f(x_i) - \gamma q_i - (\lambda - \mu) z_i\big]^+ \\ & \lambda, \mu \ge 0 \end{aligned}$$

Finally, let's eliminate the q_i variables. For a given optimal μ and λ, it is straightforward to observe that the minimizer $q^\star$ to $\gamma/2q^2 + [w - \gamma q]^+$ must lie in the set $\{0, w/\gamma, 1\}$. In particular, if $w/\gamma \le 0$, then $q^\star = 0$. If $w/\gamma \ge 1$, then $q^\star = 1$. Note here that we make use of the fact that $\gamma > 0$.

So, the optimal value of $q^\star$ to $\gamma/2q^2 + [w - \gamma q]^+$ is:

$$\xi_\gamma(w) = \begin{cases} 0 & \frac{w}{\gamma} \le 0 \\ \frac{w^2}{2\gamma} & 0 \le \frac{w}{\gamma} \le 1 \\ w - \frac{\gamma}{2} & \frac{w}{\gamma} \ge 1 \end{cases}$$

From this, the optimization problem reduces to:

$$\min_{\lambda,\mu\geq 0} \sum_{i=1}^{N} \Big(b(\lambda-\mu) + \epsilon_0(\lambda+\mu) + \xi_\gamma(f(x_i) - (\lambda-\mu)z_i) \Big)$$

This is a differentiable objective function and can be solved quickly using the projected gradient descent method (Boyd and Mutapcic, 2008). The projection step here is is taking the positive parts of λ and μ. This leads to the update rules in Algorithm 2.

What about the solution? Given λ and μ, the solution of q_i is a minimizer to;

$$\frac{\gamma}{2}q_i^2 + \big[f(x_i) - \gamma q_i - (\lambda-\mu)z_i\big]^+$$

As stated earlier, the solution is:

$$q_i = \begin{cases} 0, & f(x_i) \leq (\lambda-\mu)z_i \\ (1/\gamma)(f(x_i) - (\lambda-\mu)z_i), & \gamma(\lambda-\mu)z_i \leq f(x_i) \leq (\lambda-\mu)z_i + \gamma \\ 1, & f(x_i) \geq (\lambda-\mu)z_i + \gamma \end{cases}$$

So, we have a ramp function. This proves Theorem 1.

D Proof of Theorem 2

D.1 Optimal Unbiased Predictors

We begin by proving the following result, which can be of independent interest.

Theorem 3. *Let $f^\star = \arg\min_{f:\mathcal{X}\to\{0,1\}} \mathbb{E}[\mathbb{I}\{f(\boldsymbol{x}) \neq \boldsymbol{y}\}]$ be the Bayes optimal decision rule subject to group-wise affine constraints of the form $\mathbb{E}[w_k(\boldsymbol{x}) \cdot f(\boldsymbol{x}) \,|\, \boldsymbol{x} \in X_k] = b_k$ for some fixed partition $\mathcal{X} = \cup_k X_k$. If $w_k : \mathcal{X} \to \mathbb{R}$ and $b_k \in \mathbb{R}$ are such that there exists a constant $c \in (0,1)$ in which $p(f(x) = 1) = c$ will satisfy all the affine constraints, then $f^\star$ satisfies $p(f^\star(x) = 1) = \mathbb{I}\{\eta(x) > t_k\} + \tau_k \mathbb{I}\{\eta(x) = t_k\}$, where $\eta(x) = p(\boldsymbol{y} = 1|\boldsymbol{x} = x)$ is the Bayes regressor, $t_k \in [0,1]$ is a threshold specific to the group $X_k \subseteq \mathcal{X}$, and $\tau_k \in [0,1]$.*

Proof. Minimizing the expected misclassification error rate of a classifier f is equivalent to maximizing:

$$\begin{aligned} \mathbb{E}[f(\mathbf{x}) \cdot \mathbf{y} + (1 - f(\mathbf{x})) \cdot (1 - \mathbf{y})] &= \mathbb{E}\Big[\mathbb{E}[f(\mathbf{x}) \cdot \mathbf{y} + (1 - f(\mathbf{x})) \cdot (1 - \mathbf{y})] \,\big|\, \mathbf{x}\Big] \\ &= \mathbb{E}\Big[\mathbb{E}[f(\mathbf{x}) \cdot (2\eta(\mathbf{x}) - 1)] \,\big|\, \mathbf{x}\Big] + \mathbb{E}[1 - \eta(\mathbf{x})] \end{aligned}$$

Hence, selecting f that minimizes the misclassification error rate is equivalent to maximizing:

$$\mathbb{E}[f(\mathbf{x}) \cdot (2\eta(\mathbf{x}) - 1)] \tag{14}$$

Instead of maximizing this directly, we consider the regularized form first. Writing $h(x) = 2\eta(x) - 1$, the optimization problem is:

$$\min_{0\leq f(x)\leq 1} \quad (\gamma/2)\mathbb{E}[f(\mathbf{x})^2] - \mathbb{E}[f(\mathbf{x}) \cdot h(\mathbf{x})] \qquad \text{s.t.} \qquad \mathbb{E}[w(\mathbf{x}) \cdot f(\mathbf{x})] = b$$

Here, we focused on one subset X_k because the optimization problem decomposes into K separate optimization problems, one for each X_k. If there exists a constant $c \in (0,1)$ such that $f(x) = c$ satisfies all the equality constraints, then Slater's condition holds so strong duality holds (Boyd and Vandenberghe, 2004).

The Lagrangian is:

$$(\gamma/2)\mathbb{E}[f(\mathbf{x})^2] - \mathbb{E}[f(\mathbf{x}) \cdot h(\mathbf{x})] + \mu(\mathbb{E}[w(\mathbf{x}) \cdot f(\mathbf{x})] - b) + \mathbb{E}[\alpha(\mathbf{x})(f(\mathbf{x}) - 1)] - \mathbb{E}[\beta(\mathbf{x})f(\mathbf{x})],$$

where $\alpha(x), \beta(x) \geq 0$ and $\mu \in \mathbb{R}$ are the dual variables.

Taking the derivative w.r.t. the optimization variable $f(x)$ yields:

$$\gamma f(x) = h(x) - \mu\, w(x) - \alpha(x) + \beta(x) \tag{15}$$

Therefore, the dual problem becomes:

$$\max_{\alpha(x),\beta(x)\geq 0} -(2\gamma)^{-1}\,\mathbb{E}[(h(\mathbf{x})-\mu\,w(\mathbf{x})-\alpha(\mathbf{x})+\beta(\mathbf{x}))^2]-b\mu-\mathbb{E}[\alpha(\mathbf{x})]$$

We use the substitution in Eq. (15) to rewrite it as:

$$\min_{\alpha(x),\beta(x)\geq 0}(\gamma/2)\,\mathbb{E}[f(\mathbf{x})^2]+b\mu+\mathbb{E}[\alpha(\mathbf{x})]$$
$$\text{s.t.}\forall x\in\mathcal{X}:\gamma f(x)=h(x)-\mu\,w(x)-\alpha(x)+\beta(x)$$

Next, we eliminate the multiplier $\beta(x)$ by replacing the equality constraint with an inequality:

$$\min_{\alpha(x)\geq 0}(\gamma/2)\,\mathbb{E}[f(\mathbf{x})^2]+b\mu+\mathbb{E}[\alpha(\mathbf{x})]$$
$$\text{s.t.}\forall x\in\mathcal{X}:h(x)-\gamma f(x)-\mu\,w(x)-\alpha(x)\leq 0$$

Finally, since $\alpha(x)\geq 0$ and $\alpha(x)\geq h(x)-\gamma f(x)-\mu w(x)$, the optimal solution is the minimizer to:

$$\min_{f:\mathcal{X}\to\mathbb{R}}\ (\gamma/2)\mathbb{E}[f(\mathbf{x})^2]+b\mu+\mathbb{E}[\max\{0,\,h(\mathbf{x})-\gamma f(\mathbf{x})-\mu w(\mathbf{x})\}]$$

Next, let $\mu^\star$ be the optimal solution of the dual variable μ. Then, the optimization problem over f decomposes into separate problems, one for each $x\in\mathcal{X}$. We have:

$$f(x)=\arg\min_{\tau\in\mathbb{R}}\Big\{(\gamma/2)\tau^2+[h(x)-\gamma\tau-\mu^\star\,w(x)]^+\Big\}$$

Using the same argument in Appendix C, we deduce that $f(x)$ is of the form:

$$f(x)=\begin{cases}0, & h(x)-\mu^\star\,w(x)\leq 0\\ 1 & h(x)-\mu^\star\,w(x)\geq\gamma\\ (1/\gamma)\,(h(x)-\mu^\star\,w(x)) & \text{otherwise}\end{cases}$$

Finally, the statement of the theorem holds by taking the limit as $\gamma\to 0^+$. □

D.2 Excess Risk Bound

We use robustness-based analysis (Xu and Mannor, 2012). First, observe that the loss function that we care about is of the form (see Eq. (14)):

$$l(u,x_i)=-f(x)\cdot\tilde{f}(x_i,u),$$

where $f(x):\mathcal{X}\to[-1,+1]$ has a bounded range and $\tilde{f}$ is of the form shown in Figure 2(a). We will call a function of the form shown in Figure 2(a) a thresholding function with width $\gamma>0$. We note here that the regularization term plays the rule of making the loss class Lipschitz continuous. In general, the decision rule is of the form:

$$\tilde{f}(x)=\begin{cases}0, & \text{if } f(x)\leq\tau_{k,s}\mu_k\\ 1, & \text{if } f(x)\geq\gamma+\tau_{k,s}\mu_k\\ (1/\gamma)\,(f(x)-\tau_{k,s}\mu_k) & \text{otherwise,}\end{cases}$$

for some $|\tau_{k,s}|\leq 1$. Note here that $\tau_{k,s}$ depends on the group X_k and the sensitive class S (i.e. all instances x that belong to the same group and sensitive class have the same decision rule). In addition, observe that the decision rule depends on x only via $f(x)\in[-1,+1]$. Hence, we write $\mathbf{z}=f(\mathbf{x})$ and denote the loss by $l(u,\mathbf{z})=\mathbf{z}\cdot\tilde{f}(\mathbf{z},\,u)$. Since the thresholds are learned based on a fresh sample of data, the random variables $\mathbf{z}_i$ are i.i.d. Moreover, this loss is $2(1+1/\gamma)$-Lipschitz continuous within the same group and sensitive class.

Let $\tilde{\mu}\in\mathbb{R}^K$ be the thresholds produced by the algorithm and let $\tilde{\mathbf{h}}_\gamma$ be the resulting decision rule. Using Corollary 5 in (Xu and Mannor, 2012), we conclude that with a probability of at least $1-\delta$:

$$\big|\mathbb{E}_{\mathcal{D}}[l(\tilde{\mathbf{h}}_\gamma,\mathbf{x})]-\mathbb{E}_{\mathbf{s}}[l(\tilde{\mathbf{h}}_\gamma,\mathbf{x})]\big|\leq\inf_{R\geq 1}\Big\{\big(\frac{4}{R}(1+\frac{1}{\gamma})+2\sqrt{\frac{2(R+2K)\log 2+2\log\frac{1}{\delta}}{N}}\Big\}\qquad(16)$$

Here, we used the fact that the observations $f(\mathbf{x})$ are bounded in the domain $[-1, 1]$ and that we can first partition the domain into groups X_k with/without the sensitive class S ($2K$ subsets) in addition to partitioning the interval $[-1, 1]$ into R smaller sub-intervals and using the Lipschitz constant. Choosing $R = N^{\frac{1}{3}}$ and simplifying gives us with a probability of at least $1 - \delta$:

$$\left|\mathbb{E}_{\mathcal{D}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})] - \mathbb{E}_{\mathbf{s}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})]\right| \leq \frac{4(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 2\sqrt{\frac{3K + 2\log\frac{1}{\delta}}{N}}$$

The same bound also applies to the decision rule $\mathbf{h}^\star_\gamma$ that results from applying optimal threshold $u^\star_\gamma$ with width $\gamma > 0$ (here, "optimal" is with respect to the underlying distribution) because the ϵ-cover (Definition 1 in (Xu and Mannor, 2012)) is independent of the choice of the thresholds. By the union bound, we have with a probability of at least $1 - \delta$, both of the following inequalities hold:

$$\left|\mathbb{E}_{\mathcal{D}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})] - \mathbb{E}_{\mathbf{s}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})]\right| \leq \frac{4(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 2\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}} \tag{17}$$

$$\left|\mathbb{E}_{\mathcal{D}}[l(\mathbf{h}^\star_\gamma, \mathbf{x})] - \mathbb{E}_{\mathbf{s}}[l(\mathbf{h}^\star_\gamma, \mathbf{x})]\right| \leq \frac{4(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 2\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}} \tag{18}$$

In particular:

$$\begin{aligned}
\mathbb{E}_{\mathcal{D}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})] &\leq \mathbb{E}_{\mathbf{s}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})] + \frac{4(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 2\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}} \\
&\leq \mathbb{E}_{\mathbf{s}}[l(\mathbf{h}^\star_\gamma, \mathbf{x})] + \gamma + \frac{4(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 2\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}} \\
&\leq \mathbb{E}_{\mathcal{D}}[l(\mathbf{h}^\star_\gamma, \mathbf{x})] + \gamma + \frac{8(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 4\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}}
\end{aligned}$$

The first inequality follows from Eq. (17). The second inequality follows from the fact that $\tilde{\mathbf{h}}_\gamma$ is an empirical risk minimizer to the regularized loss, where $\mathbb{E}[\tilde{f}(\mathbf{x})^2] \leq 1$ since $\tilde{f}(x) \in [0, 1]$. The last inequality follows from Eq. (18).

Finally, we know that the thresholding rule $\mathbf{h}^\star_\gamma$ with width $\gamma > 0$ is, by definition, a minimizer to:

$$(\gamma/2)\mathbb{E}[h(\mathbf{x})^2] - \mathbb{E}[h(\mathbf{x}) \cdot f(\mathbf{x})]$$

among all possible bounded functions $h : \mathcal{X} \to [0, 1]$ subject to the desired fairness constraints. Therefore, we have:

$$(\gamma/2)\mathbb{E}[\mathbf{h}^\star_\gamma(\mathbf{x})^2] - \mathbb{E}[\mathbf{h}^\star_\gamma(\mathbf{x}) \cdot f(\mathbf{x})] \leq (\gamma/2)\mathbb{E}[\mathbf{h}^\star(\mathbf{x})^2] - \mathbb{E}[\mathbf{h}^\star(\mathbf{x}) \cdot f(\mathbf{x})]$$

Hence:

$$\mathbb{E}_{\mathcal{D}}[l(\mathbf{h}^\star_\gamma, \mathbf{x})] = -\mathbb{E}[\mathbf{h}^\star_\gamma(\mathbf{x}) \cdot f(\mathbf{x})] \leq \gamma + \mathbb{E}_{\mathcal{D}}[l(\mathbf{h}^\star, \mathbf{x})]$$

This implies the desired bound:

$$\mathbb{E}_{\mathcal{D}}[l(\tilde{\mathbf{h}}_\gamma, \mathbf{x})] \leq \mathbb{E}_{\mathcal{D}}[l(\mathbf{h}^\star, \mathbf{x})] + 2\gamma + \frac{8(2 + \frac{1}{\gamma})}{N^{\frac{1}{3}}} + 4\sqrt{\frac{3K + 2\log\frac{2}{\delta}}{N}}$$

Therefore, we have consistency if $N \to \infty$, $\gamma \to 0^+$ and $\gamma N^{\frac{1}{3}} \to \infty$. For example, this holds if $\gamma = O(N^{-\frac{1}{6}})$.

So far, we have assumed that the output of the original classifier coincides with the Bayes regressor. If the original classifier is Bayes consistent, i.e. $\mathbb{E}[|2\eta(\mathbf{x}) - 1 - f(\mathbf{x})|] \to 0$ as $N \to \infty$, then we have Bayes consistency of the post-processing rule by the triangle inequality.

E PROOF OF PROPOSITION 2

Proof. Since $|z(x)| \leq 1$ and $|\xi'_\gamma(w)| \leq 1$, the gradient at a point $\mathbf{x}$ is always bounded by $||\nabla_t||_2^2 \leq (1+\epsilon_0+b)^2$ at all rounds. Following the proof steps of (Boyd and Mutapcic, 2008) and using the fact that projections are contraction mappings, one obtains:

$$\frac{1}{T}\sum_{t=1}^{T}\left(\mathbb{E}[F^{(t)}] - F(\mu^\star)\right) \leq \frac{||\mu^\star||_2^2 + ||\gamma^\star||_2^2 + (1+\epsilon_0+b)^2 T\alpha^2}{2T\alpha}$$
$$= \frac{(1+\epsilon_0+b)^2\alpha}{2} + \frac{||\mu^\star||_2^2 + ||\gamma^\star||_2^2}{2T\alpha}$$

By Jensen's inequality, we have $\frac{1}{T}\sum_{t=1}^{T}\mathbb{E}[F^{(t)}] \leq \mathbb{E}[F(\bar{\mu})]$. Plugging this into the earlier results yields:

$$\mathbb{E}[\bar{F}] - F(\mu^\star)\big) \leq \frac{(1+\epsilon_0+b)^2\alpha}{2} + \frac{||\mu^\star||_2^2 + ||\gamma^\star||_2^2}{2T\alpha}$$

□