Biased Models Have Biased Explanations

Aditya Jain¹, Manish Reddy¹, Joydeep Ghosh¹
¹University of Texas at Austin
adityajain93@utexas.edu, manishreddy@utexas.edu, jghosh@utexas.edu

Abstract
We study fairness in Machine Learning (FairML) through the lens of attribute-based explanations generated for machine learning models. Our hypothesis is: Biased Models have Biased Explanations. To establish that, we first translate existing statistical notions of group fairness and define these notions in terms of explanations given by the model. Then, we propose a novel way of detecting (un)fairness for any black box model. We further look at post-processing techniques for fairness and reason how explanations can be used to make a bias mitigation technique more individually fair. We also introduce a novel post-processing mitigation technique which increases individual fairness in recourse while maintaining group level fairness.

1 Introduction
As Machine Learning (ML) models become more pervasive in our society, fairness of ML models has been a growing concern (Holstein et al. 2019). In numerous cases, ML models have introduced new bias or amplified existing bias present in the data (Dwork et al. 2012). Domains in which fairness in ML systems is important include criminal justice systems, chatbots, job hiring and loan approvals. In such systems, a specific type of unfairness is considered: discrimination based on a protected attribute such as race, gender or age. A widely publicized example is COMPAS (Larson et al. 2016), where the algorithm used to predict recidivism scores for defendants had a higher false positive rate for African American defendants as compared to Caucasian defendants. In this paper, we will focus on this specific notion of (un)fairness: discrimination. Future references to fairness in this work refer to discrimination based on a protected attribute. We will also be using bias to highlight discrimination. For example, a model is discriminatory when its outcomes are biased with respect to a particular protected attribute (for example, race).

Explainable AI (XAI) and Fairness
The motivation for using explanations to define discrimination is based on the hypothesis: Biased models have biased explanations. The fields of XAI and FairML have progressed independently for the past few years. A notable exception is Caruana (Caruana 2019) which uses Generalized Additive Models with interactions terms (GA2M) to highlight bias in the COMPAS dataset (Larson et al. 2016). Specifically, Caruana calculates global importance of race in determining a positive model prediction and identifies bias by comparing importance given to race feature across individuals of different races.

In this work, we present a stronger and broader connection between the fields of XAI and FairML. Lage et. al. (Lage et al. 2019) argue that XAI techniques are designed for specific downstream tasks that they help accomplish. A common and widespread downstream task is replicating model output given the explanations. Expanding on that view, we propose two tasks in FairML which can be accomplished using XAI techniques:

1. Detection of discrimination: Numerous normative definitions for quantifying discrimination exists within the literature. In this paper, we consider some of the most widely used discrimination criteria such as: demographic parity, equality of opportunity and equalized odds and propose a novel discrimination detection algorithm using attribute-based explanations.

2. Mitigation of discrimination: Three classes of techniques exist for mitigation of discrimination: pre-processing, in-processing and post-processing techniques, categorized on the basis of where the intervention is performed in the modeling pipeline. Post-processing techniques are suitable for run-time environment, require no knowledge of training process, model architecture, internal weights or derivatives and thus are applicable to any black-box model setting. In this work, we will propose a novel post-processing method using attribute-based explanations.

With a increasing number of XAI techniques available, some natural questions arise: Which XAI technique would be most suited for each of the FairML tasks, Is there a single XAI technique which can be used effectively for all of the above tasks. While, we believe there is no one correct answer (or technique) for each of these tasks and choosing
one is more art than science, we propose SHapley Additive exPlanations (SHAP Values) (Lundberg and Lee 2017) as an excellent choice to accomplish aforementioned FairML tasks of detection and mitigation of bias. The key contributions of this paper are:

- Relate fields of XAI and FairML by proposing techniques to guide bias detection and mitigation using attribute-based explanations.
- Introduce a novel discrimination detection method using SHAP explanations.
- Propose a novel post processing algorithm to achieve increased individual fairness with baseline group fairness guarantees as provided by Pleiss et. al. (Pleiss et al. 2017)

2 SHAP Values: Background and Merits

SHAP (SHapley Additive exPlanations) values provide a unified framework for explaining the output of a complex model $f(x)$ for an individual observation $x$ based on the attributes present in $x$. SHAP assigns a score (SHAP Value) to each feature corresponding to the contribution of that feature for a particular prediction. The sum of all SHAP Values plus a constant mean score is equal to the prediction score for that observation. Mathematically, SHAP values are represented by,

$$φ_i(f, x) = ∑_{z \in \mathbb{I}} \frac{|z|!}{M!} \left[ f(x) - f(x \setminus i) \right]$$ (1)

where $φ_i$ represents the SHAP value for a function $f$, input $x$ and feature $i$. The prediction $f(x)$ can then be written as

$$f(x) = φ_0 + ∑_M φ_i(x)$$ (2)

where $M$ is number of active input features and $φ_i \in R$. Refer to Lundberg et. al (Lundberg and Lee 2017) for more details. The merits of choosing SHAP Values for downstream FairML tasks are:

- SHAP Values have strong theoretical basis in game theory and obey properties of Local Accuracy, Missingness and Consistency (Lundberg and Lee 2017).
- SHAP values quantify explanations by having both magnitude and direction. This helps define statistical discrimination criteria using local explanations.
- SHAP values offer global explanations that are consistent with atomic local explanations unlike, say, LIME (Ribeiro, Singh, and Guestrin 2016)

3 Defining discrimination using SHAP values

Earlier, we briefly mentioned popular discrimination criteria used in the literature, namely: demographic parity, equality of opportunity and equalized odds. Below, we translate them in terms of SHAP explanations, model score (R) and true outcome (Y) for a protected attribute (A).

**Demographic Parity** is defined as the independence of the protected attribute (A) and the model score (R) i.e. $R \perp A$ (Barocas, Hardt, and Narayanan 2018). The protected attribute should have neither a positive or a negative contribution towards the prediction. Equivalently, it can be defined as the SHAP value of protected attribute (A) having a negligible magnitude. Therefore to check if a model complies to the notion of demographic parity, we consider the mean absolute SHAP values for the protected attribute(A).

A mean absolute SHAP value significantly away from zero would indicate violation of demographic parity.

**Equality of Opportunity** requires that a qualified individual (Y=1) should have equal chances of being assigned a favourable outcome regardless of their protected attribute (Hardt et al. 2016). Mathematically, it can be expressed as $R \perp A | Y = 1$ (Barocas, Hardt, and Narayanan 2018).

In terms of SHAP explanations, it implies that the distribution of SHAP Values of the protected attribute (A) for true advantageous outcome (Y=1) should be similar. Similarity of distribution here can be defined in terms of KL Divergence (Shlens 2014) or Wasserstein’s distance (Ramdas, Trillos, and Cuturi 2017).

**Equalized Odds or Separation** is defined as the independence between the model score (R) and the protected attribute (A) to the extent justified by the target outcome or $R \perp A | Y$ (Barocas, Hardt, and Narayanan 2018). It can be seen as an extension of Equality of Opportunity with independence between R and A for both Y=1 and Y=0.

In terms of SHAP Values, given a particular true outcome (Y), the SHAP explanation for the protected attribute should be similar for different protected classes. The similarity for these distributions can be measured in terms of KL Divergence (Shlens 2014) or Wasserstein’s distance (Ramdas, Trillos, and Cuturi 2017).

4 Detecting discrimination using SHAP values

The above definitions form the basis of the proposed discrimination detection method. The inputs to the method are:

- **Input dataset D**: Dataset containing input features (X) and true outcome (Y) for all data points.
- **Model M**: ML model provides soft (model score R) or hard predictions (model outcome Ŷ) on Input dataset D
- **Discrimination criterion C**
- **Protected Attribute A**

The output is to detect and quantify discrimination of model M on protected attribute A as seen for input dataset D and as measured by the criterion C. The detection technique can be divided into three steps.

**STEP 1: Calculate SHAP Values**

Contingent on the level of access we have to the model M, there exists two techniques to calculate SHAP values for the input dataset D:
• **White Box Setting**: assumes complete knowledge and access to model type and internal parameters. In this case, depending on the model type, we leverage different computationally efficient techniques mentioned in Lundberg et al. (Lundberg and Lee 2017) to calculate SHAP values for different model types. (In practice, this would be the case when we ourselves are the producers of the ML model.)

• **Black Box Setting**: Here, our access to the model is limited: we have no information about model type or internal parameters. We do, however, have access to a model API which gives us the prediction for a given input. We query the model API for predictions for all points in the input dataset. Next, we create a mimic or student model S to learn the decision boundary of the original model M, a technique referred to as distillation (Tan et al. 2018). We do this by training the model on the input features (X) to predict the model score generated by Model M. Depending on the output of the model API, the mimic model could minimize (1) cross entropy loss if the API for model M gives an output class (Y) as the prediction or (2) mean squared error if the API returns a model score (R) as a prediction. Finally, we use the mimic model to calculate SHAP Values for the input dataset D using the appropriate technique as mentioned in Lundberg et al. (Lundberg and Lee 2017).

A natural question to ask: What hypothesis class to choose for the mimic model? While again, there is no right choice, we chose Gradient Boosted Trees (XGBoost (Chen and Guestrin 2016) specifically) due to their high expressiveness, generalizability and existence of a computationally efficient mechanism to compute SHAP Values, namely TreeSHAP (Lundberg, Erion, and Lee 2018). There could be other hypothesis classes which might work well for different problems. It would be interesting to consider how the choice of mimic model affects FairML tasks. We leave this experimentation for future work.

**STEP 2: Quantify Discrimination**

After calculating SHAP values for all data points in the input dataset, we use SHAP values of the protected attribute to detect and quantify discrimination. The SHAP equivalent definition of discrimination criteria described in Section 3 compares the distributions of SHAP values of the protected attribute for different slices in the dataset. For example Equality of Opportunity compares distribution of SHAP Values of protected attribute (A) for Y=1, A=a and Y=1, A=b where a,b are two values realised by protected attribute. To quantify discrimination, we can look at different measures to compare distributions. Some popular methods include Wasserstein’s distance (Ramdas, Trillos, and Cuturi 2017), Kullback–Leibler divergence (Shlens 2014) and mutual information (Kraskov, Stögbauer, and Grassberger 2004).

**STEP 3: Establish a fairness baseline**

We randomize values of the protected attribute (A) preserving the original proportions of each class, to establish a baseline to compare the chosen discrimination criterion. As we will see, randomization confounds the model to an extent and serves as the baseline to compare quantified discrimination measures.

### 5 Case Study: COMPAS Dataset

We tested the proposed discrimination detection algorithm on ProPublica’s COMPAS recidivism dataset (Larson et al. 2016) and identified whether it violated the aforementioned discrimination criteria with race as the protected attribute. We followed the same data pre-processing steps taken in Propublica’s original analysis (Larson et al. 2016). Here, since we do not have access to the original model used in COMPAS (thus, black-box problem setting), we used distillation to create a mimic model from the dataset. We used gradient boosted trees as implemented in the XGBoost library in python to perform a binary classification with Y=1 representing a Low recidivism score i.e. a favourable outcome. The AUC score of the trained model was 0.83. The trained model was then used to calculate SHAP values for different input features using TreeSHAP (Lundberg, Erion, and Lee 2018), a computationally efficient method to calculate SHAP values for tree-based models. To establish a baseline for comparison, we also created a randomized race feature by randomly permuting the race while preserving the total number of people in each race.

**Detecting Discrimination**

![Figure 1: Distribution of SHAP values for race and randomized race (baseline)](image)

**Demographic Parity**  
A model unbiased on protected attribute A and based on criterion of demographic parity has negligible contribution (SHAP Value) of protected attribute . Fig. 1 shows the distribution of SHAP values for race and randomized race baseline. The impact of randomized race on the model is negligible with a mean absolute SHAP value of 0.01 while race has a bi-modal distribution of SHAP values with a significant non-zero absolute mean of 0.05. A deeper examination shows that being Caucasian increases an individual odds of being assigned a favourable outcome (lower recidivism score) and being African American affects the individual negatively.

**Equality of Opportunity**  
requires the distribution of SHAP value of protected attribute for both races to be simi-
lar given the individual did not re-offend (Y=1). The SHAP value distributions of African Americans and Caucasians are substantially different with different mean values. On the other hand, a random race assignment leads to a more similar distribution of SHAP values. Table 1 specifies the Wasserstein’s distance between the distributions.

### Table 1: Wasserstein’s distance between SHAP contribution of Caucasians and African-Americans for different slices of dataset based on true outcome and randomization

| Race          | Randomized Race |
|---------------|-----------------|
| Y = 0         | 0.110           |
|               | 0.010           |
| Y = 1         | 0.100           |
|               | 0.012           |

### 6 Fairness Recourse Using SHAP Values

Biased Machine Learning models have penetrated many critical decision making processes in the society. To make these models less discriminatory, three classes of techniques exist: pre-processing, in-processing and post-processing techniques, categorized on the basis where the intervention is performed in the modeling pipeline. As mentioned earlier, post-processing techniques have numerous advantages and we will use SHAP values to enhance existing post-processing techniques.

#### Motivation for using SHAP values for Recourse

In order to achieve group fairness (according to a particular fairness metric, say Equalized Odds), two notable post-processing technique proposed in Pleiss et al. (Pleiss et al. 2017) and Hardt et al. (Hardt et al. 2016) exist. Both these techniques use a randomization step which changes the predictions in either one of the following ways: Predictions (which are biased) of some randomly selected members of the advantaged group are flipped (Hardt et al. 2016) or set to the base rate (Pleiss et al. 2017). The loss in accuracy in post-processing techniques is in line with the fairness-accuracy trade off discussed extensively in the (Pleiss et al. 2017), (Hardt et al. 2016)) and widely accepted in the community.

To motivate the use of SHAP values for recourse, we use the concept of Shapley Values (Shapley ) as studied in the field of game theory. Shapley Values define a fair payout strategy in a game consisting of multiple players with different skill sets and a total reward that the group achieved by playing the game. Now, consider model score (R) for an individual (equivalently data point) is the reward received in a game. For different individuals, input features contribute differently towards the attained reward. SHAP values give us this contribution and discrimination (or bias) occurs when a particular group of individuals is awarded extra credit by being part of the advantaged group, say belonging to a particular race. We would ideally want the reward earned due to race to be zero or similar for different types of races. To correct this, post-processing techniques penalize rewards (thus, lose accuracy) of random individuals from an advantaged group so that finally, rewards of the advantageous and disadvantageous groups as a whole are fair (according to the predetermined group fairness metric).

We propose an alternate approach to select individuals to be penalized which uses SHAP values to choose individuals (data points) instead of randomly selecting them. As described before, SHAP values give us the contribution of the protected attribute towards attaining a particular model score $R$ (equivalently reward). Instead of randomly redistributing rewards from individuals of an advantaged group, we propose to use SHAP values of the protected attribute (say race) to arbitrate how to redistribute the reward and achieve group fairness. The redistribution method is depends on the post processing algorithm used and an example of it will be discussed in the next section.

Consider the toy example described in Table 2. Individuals A and B received undue advantage for a favourable outcome due to their membership to an advantageous protected
attribute. To mitigate that, we penalize their predictions (or equivalently reward) and choose between either Individual A or B to decrease their prediction and decrease the undue advantage of advantageous class. Here, Individual A has a higher contribution of race (0.3) as compared to Individual B (0.1). They both have the same prediction of 0.9 towards a favourable outcome. Rather than randomly choosing either individual, we use SHAP values of features other than race to make an individually fair choice. We can see that Individual A is less skilled/able/deserving for a positive outcome than Individual B. So we should choose Individual A’s prediction to be decreased. This toy example can be extended to existing post-processing techniques to achieve higher levels of individual fairness maintaining group fairness criteria.

We operationalize the above post-processing mitigation blueprint by first calculating SHAP values. Based on the problem at hand, one could have access to the whole model, its parameters and architecture, the white-box setting as described earlier. On the other hand, in the black-box setting, one may only have access to the model API which can be queried to generate a labeled dataset to train a mimic model, a technique known as distillation (Tan et al. 2018). Once we have a classification model, the SHAP values for the dataset can be found out using the techniques described in Lundberg et al. (Lundberg and Lee 2017). The SHAP values give us the ability to intelligently process predictions to satisfy a group fairness measure while increasing individual fairness. The exact algorithm depends on the post-processing technique used. The idea of using SHAP values for fairness is adaptable to multiple post-processing techniques and objectives, an example of which will be discussed in the following section.

### 7 Post Processing Fairness on a Calibrated Classifier using SHAP

_Pleiss et al. 2017_ consider calibrated probability estimates as essential when these estimates are used in downstream decision-making tasks. Apart from the innate biases present in the human decision-making, in practical settings, an uncalibrated classifier gives more incentive to the decision maker to mistrust the predictions and increasingly rely on their own judgements solely. In their paper _On Fairness and Calibration_, Pleiss et al. 2017 prove that model calibration is only compatible with a single group fairness constraint. To combat that, they suggest a weighted cost to incorporate multiple group fairness metrics. The weighted cost serves as a fairness constraint across different classes. In order to equalize this cost, they suggest a post processing fairness algorithm which randomly selects individuals from a group with lower error costs (advantageous class) and arrives at a calibrated fair classifier $h'_t$ which is

$$
h'_t(x) = \begin{cases} 
    \mu_t & \text{with probability } \alpha \\
    h_t(x) & \text{with probability } 1 - \alpha 
\end{cases}
$$

$t$: protected group whose predictions are changed
$\mu_t$: new classifier for protected group $t$
$h_t$: original classifier for protected group $t$
$\alpha$: randomization rate

#### Calibrated Post Processing using SHAP values

The calibrated post processing algorithm in _Pleiss et al. 2017_ calculates a randomization rate $\alpha$ for a particular protected group $t$ at which predictions of certain individuals are set to the base rate of the protected group $t$. These individuals will have varied predictions and SHAP values (contributions) of the protected attribute. The space of all $\text{contribution} \times \text{prediction}$ can be divided into 4 quadrants as shown in the Fig. 4. The semantic meaning of these regions is:

- **Quadrant 1**: (prediction $>$ base rate) and (contribution of protected attribute $>$ 0). These individuals benefited due to the protected attribute. The positive contribution of the protected attribute could have pushed certain non-deserving individuals towards a positive outcome.
- **Quadrant 2**: (prediction $>$ base rate) and (contribution of protected attribute $<$ 0).
- **Quadrant 3**: (prediction $<$ base rate) and (contribution of protected attribute $>$ 0). These individuals were affected the most since they could have had a positive prediction if not for a negative contribution of the protected attribute.
- **Quadrant 4**: (prediction $<$ base rate) and (contribution of protected attribute $<$ 0).

An example of the different quadrants for the COMPAS dataset is in Fig 4. One can choose different distance functions to categorize individuals in the 2-D plane of contributions of protected attribute and predictions ($\text{shap} \times \text{pred}$) with the origin set at (0, base rate). Some examples are

- Contribution of the protected attribute ($\text{shap}$)
- Contribution of all features except the protected attribute ($\text{pred} - \text{shap}$)

The algorithm first picks individuals from $(\text{quadrant}_1 \cup \text{quadrant}_4)$ who have the largest distance. If there are more individuals left, it picks individuals from $(\text{quadrant}_2 \cup \text{quadrant}_3)$ having the least distance. The core idea is to correct the individuals most affected from bias in the classifier (either favourably or unfavourably).

- **Quadrant 1** represents individuals getting the largest advantage due to a protected attribute.

| Individual A | SHAP Values of Features | Individual B |
|--------------|-------------------------|--------------|
| 0.3          | Race                    | 0.1          |
| 0.1          | Income                  | 0.3          |
| 0.1          | Age                     | 0.1          |
| 0.4          | Mean                    | 0.4          |
| 0.9          | Model Score             | 0.9          |

Table 2: SHAP Values for two individuals A and B who belong to an advantageous class.
### 8 Conclusion and Future Work

SHAP values provide an excellent bridge between XAI and FairML. Using SHAP values, we were able to detect discrimination and provide recourse using the calibrated post-processing technique mentioned in (Pleiss et al. 2017) with
improved individual fairness results. We believe that the usefulness of XAI to improve FairML tasks extends beyond SHAP Values. Multiple exciting directions for the future work exist:

• **XAI Methods:** Experiment with other local XAI methods and study their usefulness for downstream FairML tasks.

• **FairML Tasks:** Look at other post-processing fairness techniques (for example (Hardt et al. 2016)) and use XAI methods to make them more individually fair. Another interesting direction could be consider in-processing techniques and reason how XAI methods can help improve them.

• **Individual Fairness:** Define a measure for individual fairness and directly optimize for it.

**References**

Barocas, S.; Hardt, M.; and Narayanan, A. 2018. Fairness and machine learning. fairmlbook.org.

Caruana, R. 2019. Friends don’t let friends deploy black-box models: The importance of intelligibility in machine learning. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, KDD ’19, 3174. New York, NY, USA: Association for Computing Machinery.

Chen, T., and Guestrin, C. 2016. Xgboost: A scalable tree boosting system. In Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining, 785–794. ACM.

Dwork, C.; Hardt, M.; Pitassi, T.; Reingold, O.; and Zemel, R. 2012. Fairness through awareness. In Proceedings of the 3rd innovations in theoretical computer science conference, 214–226. ACM.

Hardt, M.; Price, E.; Srebro, N.; et al. 2016. Equality of opportunity in supervised learning. In Advances in neural information processing systems, 3315–3323.

Holstein, K.; Wortman Vaughan, J.; Daumé III, H.; Dudík, M.; and Wallach, H. 2019. Improving fairness in machine learning systems: What do industry practitioners need? In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 600. ACM.

Kraskov, A.; Stögbauer, H.; and Grassberger, P. 2004. Estimating mutual information. Physical review E 69(6):066138.

Lage, I.; Chen, E.; He, J.; Narayanan, M.; Kim, B.; Gershman, S.; and Doshi-Velez, F. 2019. An evaluation of the human-interpretabiliy of explanation. CoRR abs/1902.00006.

Larson, J.; Mattu, S.; Kirchner, L.; and Angwin, J. 2016. How we analyzed the compas recidivism algorithm. ProPublica (5 2016) 9.

Lundberg, S. M., and Lee, S.-I. 2017. A unified approach to interpreting model predictions. In Advances in Neural Information Processing Systems, 4765–4774.

Lundberg, S. M.; Erion, G. G.; and Lee, S.-I. 2018. Consistent individualized feature attribution for tree ensembles. arXiv preprint arXiv:1802.03888.

Pleiss, G.; Raghavan, M.; Wu, F.; Kleinberg, J.; and Weinberger, K. Q. 2017. On fairness and calibration. In Advances in Neural Information Processing Systems, 5680–5689.

Ramdas, A.; Trillos, N.; and Cuturi, M. 2017. On wasserstein two-sample testing and related families of nonparametric tests. Entropy 19(2):47.

Ribeiro, M. T.; Singh, S.; and Guestrin, C. 2016. Model-agnostic interpretability of machine learning.

Shapley, L. S. A value for n-person games.

Shlens, J. 2014. Notes on kullback-leibler divergence and likelihood. arXiv preprint arXiv:1404.2000.

Tan, S.; Caruana, R.; Hooker, G.; and Lou, Y. 2018. Distill-and-compare: auditing black-box models using transparent model distillation. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, 303–310. ACM.