Contrastive Examples for Addressing the Tyranny of the Majority

Viktoriia Sharmanska  
Imperial College London

Lisa Anne Hendricks  
DeepMind*

Trevor Darrell  
UC Berkeley

Novi Quadrianto  
University of Sussex

Abstract

Computer vision algorithms, e.g. for face recognition, favour groups of individuals that are better represented in the training data. This happens because of the generalization that classifiers have to make. It is simpler to fit the majority groups as this fit is more important to overall error. We propose to create a balanced training dataset, consisting of the original dataset plus new data points in which the group memberships are intervened, minorities become majorities and vice versa. We show that current generative adversarial networks are a powerful tool for learning these data points, called contrastive examples. We experiment with the equalized odds bias measure on tabular data as well as image data (CelebA and Diversity in Faces datasets). Contrastive examples allow us to expose correlations between group membership and other seemingly neutral features. Whenever a causal graph is available, we can put those contrastive examples in the perspective of counterfactuals.

1 Introduction

Figure 1 illustrates the concept of the tyranny of the majority [11, 25] in algorithmic decisions. The goal is to predict the income of an individual, without becoming unfairly biased by gender. The x-axis shows how consistently increasing the number of women in the training set, until the number of men and women is equal, leads to higher accuracy, as well as fairer predictions. We measure fairness with several metrics (difference in true positive rate, false positive rate, acceptance rate, positive predicted value, and negative predicted value between males and females; lower is better for all fairness metrics), and consistently see improved performance as the dataset becomes more balanced. In all cases the proportion of high/low income individuals remains constant. Though we can analyze the impact of the tyranny of the majority in a controlled scenario, real data is rarely balanced in

*Work done at UC Berkeley
such a way. In contrast, real data reflects a variety of biases including inequality, exclusion, or other forms of inequality. The danger is that biases in the training data result in machine learning-based decisions that perpetuate these biases. Biased machine learning systems lead to decisions that are allocatively harmful [4] to certain individuals because they receive less favourable opportunities (e.g. a loan, an interview) than others. Using personal data to perpetuate biased decision making is illegal if data refer to personal characteristics that are protected under anti-discrimination legislation, such as, racial origin, gender. Furthermore, we continue to expect our AI systems to perform more and more complex tasks, such as facial recognition for law enforcement [20], or job screening via video interviews (https://www.hirevue.com/). Such tasks require building systems which can operate over complex, high dimensional visual inputs while remaining fair and lawful.

The machine learning community is actively responding to these bias in, bias out problems under the topic of fairness in machine learning. There are several ways to enforce fairness in machine learning models, before the model training phase as a pre-processing step (our method belongs here), during the model training phase, or after the model training phase as a post-processing step. Early approaches in fairness models pre-process either the target labels by reweighting [28], or the features of the data [50]. The aim of reweighting is to remove the statistical dependence between the protected attribute and the label. Recently, [1] generalize this reweighting method for any definition of fairness that can be formalized via linear inequalities on conditional moments, such as demographic parity (equality of acceptance rates) or equalized odds (equality of true and false positive rates). [50] pre-processed the features of the data points by transforming them into a latent space. Recent advances in learning fair representations suggest adversarial training [21] as the means to hide the protected characteristics from the classifier, e.g. [6, 48, 51, 33].

In this paper, we propose a simple de-biasing framework that redefines the reweighting approach based on the concept of intervention or manipulation. We reweight the original training dataset in which each data point is used twice (for binary protected attributes), however, the second copy is a counterfactual data point by intervening the protected attribute. A counterfactual is equivalent to an imaginary intervention on a causal model in which all variables that are not affected by the intervention are assumed to stay at the current observed levels. Unfortunately, for many applications, we do not have causal models about how the data were generated. Instead of counterfactuals that rely on a set of non-testable causal assumptions such as causal graphs and corresponding structural equations, we refer to the data points with intervened protected attributes as contrastive examples. To begin with, the contrastive examples can be produced using a statistical matching technique (see for example [39]), i.e. for every data point, we find one or more datapoints with similar observable features and the same target label yet having an opposite protected attribute value. The empirical performance of this matching approach depends on the choice of observable features that act as control variables, and the similarity metric. As an alternative, we show that current generative adversarial networks are able to synthesize those contrastive examples. Instead of using adversarial learning to remove protected attributes from data as done in all previous work, we use them to generate data points with pre-specified protected attributes. For non-binary protected attributes (e.g. race), each data point will have as many contrastive samples as number of values. As an added bonus, contrastive examples can be easily interpreted because they have the semantic meaning of the input (see Figures 3 and 4). If we want to encourage public conversations regarding fair machine learning systems, interpretability in fairness is an integral ingredient. As well, contrastive examples can facilitate rejection learning [12, 13], allowing models to reject (not make a prediction) if there is no output agreement between original and contrastive examples.
Related work  For completeness, we also review methods that enforce fairness during and after training. To target fairness during training, many methods add fairness terms as constraints to the classifier learning objective function (e.g. [29, 49, 37]). The resulting constrained optimisation problem can be turned into a regularised optimisation problem by making use of its Lagrangian dual form, in which the fairness constraints are moved to the objective and act as a regularizer. The Lagrangian dual variable in front of the fairness regularizer determines the trade-off between fairness and accuracy. Methods for ensuring fairness via a post-processing step, after model training is done, are also available. Having access to binary predictions or continuous scores, [24] utilise multiple-threshold rules, where each sub-group has its own threshold, to enforce fairness. Though, by having different thresholds for different sub-groups, we suffer from the disparate treatment [5], as the classifier makes its predictions based on protected attributes. Hence there is also a tension between using [24] and not using [49, 37] protected attributes as part of an input to the classifier.

In our work, we intervene on training samples to build a better dataset. Intervention has also been used at test time to interpret/explain AI systems. For example, [46] consider generation of counterfactual explanations for classification tasks for tabular input data (data is a vector of various attributes such as gender or race). After training a model, [46] generate counterfactuals by optimising for a data point which is similar to an input datapoint but yields a different outcome. Though also considering counterfactual/contrastive examples, our work is fundamentally different because we consider using contrastive examples during training to build better models and our method for generating contrastive examples (nearest neighbour-based and GANs-based) can be applied to more complex input data e.g., natural images. Other work in explainable AI aims to discover causal relationships [36, 30] in machine learning models through intervention on test samples (e.g., blocking out an object in an image), and observing how the output changes. We believe that our contrastive examples can also serve as a kind of explanation, both by allowing us to visually observe the difference between original and contrastive examples and by allowing us to understand how outcomes change if a model is provided with a contrastive example.

Recently a few representation learning methods have addressed algorithmic fairness in computer vision [38, 41]. In [38], the learned representation is made independent from the protected attribute via Hilbert-Schmidt independence criterion (HSIC). In [41], Sattigeri et al translate the data into a new image-like domain, where the demographics dependency is removed via adversarial network training. In computer vision, bias due to gender or ethnicity has been addressed via collecting large diverse datasets [34, 2, 47] and via learning a domain invariant representation [19]. Alvi et al [2] define domains as demographic groups and learn image representation that is confused about gender and/or ethnicity using domain confusion [44]. Ryu et al [40] explore a two-stage procedure: first learning the demographics representation from an external dataset, and then learning the classifier based on image and demographic representations. This approach comes at risk of indirect discrimination, i.e. indirectly conditioning the classification on protected characteristics. Wang et al [47] learn to transfer knowledge from Caucasian (source) domain to other-race (target) domains via the maximum mean discrepancy (MMD) criterion. However, this approach comes with an unethical decision which race to transfer the knowledge from. Domain adaptation methods solve distribution mismatch between training and deployment time and do not enforce fairness. Our work is also related to prior works in which generative models have been used to create additional data for domain adaptation [43, 27, 44], and to model regression tasks such as age progression [52]. However, our goal is different as we aim to build fair systems and utilize contrastive examples to gain insight into our model’s behavior.
Figure 2: We introduce the “ideal” dataset that addresses the tyranny of the majority in a real world dataset (left). A favourable label refers to, for example, getting a loan. The ideal dataset contains an imaginary data point for each person, i.e. the one inside the black box, whereby we intervene and set the gender attribute to the opposite that is in real life. In this paper, we describe two approaches to produce these contrastive data points: a generative adversarial network (GAN)-based approach and a nearest neighbour (NN) matching based on a set of features (right). While NN contrastive examples are a real person, GAN contrastive examples are not.

2 The “Ideal” Dataset

As in the vast majority of fairness in machine learning literature, we focus on the task of batch classification. An “ideal” training dataset is a dataset that for each data point with the corresponding target label, we have an imagined (contrastive) version of it with the protected attribute value, such as gender, is set to the opposite that is in real life while retaining the original target label (Figure 2–left). An ideal dataset will produce AI system behaviour that is intuitively fair. Suppose we have an AI system that is used to produce shortlisted candidates. If we had a female applicant and she was invited to the interview, had she been a male, she would have also been invited to the interview. The same should hold for male applicants. Note that an ideal dataset does not affect the distribution of the target label (invited/not invited), but balances group representations within the class (the same amount of females and males got invited/not invited). On the other hand, in fairness work, a dataset is called perfect if the base acceptance rate is the same for both groups, that is target label is independent of protected attribute. If this perfect dataset condition holds, demographic parity and equalized odds can be satisfied simultaneously [31, 10]. The main hypothesis of this paper is that our ideal dataset with contrastive examples is in fact a perfect dataset, and thus fairness definitions are not mutually exclusive. The challenge is that we do not have the previously described ideal dataset much in the same way as we can not conduct an “ideal” experiment in a study to understand the effect of a particular treatment or exposure [45]. The term ideal dataset is inspired by the concept of an ideal experiment that requires going back in time and intervening on the treatment, but we can also call it a balanced dataset; the two terms can be used interchangeably. In this paper, we describe two approaches to produce contrastive data points for generating an ideal dataset: a generative adversarial network (GAN)-based approach and a nearest neighbour (NN) matching based on a set of features (Figure 2–right). We will now detail the GAN-based approach.
One of the best models to perform image-to-image translation between image domains of different semantic attributes is StarGAN [9]. StarGAN does not require paired images for training and is suitable for learning multi-domain translation. Fairness models are typically studied using tabular datasets such as e.g. the Adult Income dataset from the UCI repository [15]. Next we describe how the StarGAN model can be successfully adapted for synthesis in tabular datasets.

**Data-to-data translation with StarGAN.** The StarGAN model consists of two components: a conditional data generator \( G \) and a discriminator \( D \). Given an input sample \( x \), and a target sensitive attribute \( s \), the generator transforms \( (x, s) \) into a synthesized contrastive image \( \hat{x} \), which preserves the content of \( x \) while changing the target sensitive attribute. For example, if gender is a protected attribute, for each male sample we create a contrastive example by conditioning the mapping on the female attribute as a target characteristic. The input to the generator \( (x, \bar{s}) \) is a depth-wise concatenation of the original \( x \) and the spatially replicated target label \( \bar{s} \) as an extra channel. If the input sample is \( 224 \times 224 \times 3 \) (RGB image), the concatenated input will become \( 224 \times 224 \times 4 \); similarly, if the input is \( 62 \times 1 \) (tabular data), the concatenated input to the generator will be \( 62 \times 2 \). In case of multiple sensitive attributes, we will add them as extra channels. The structure of the generator network follows closely the original StarGAN architecture for image data while replacing 2D convolutions with 1D convolutions for tabular data, and redefining the instance normalization and the output accordingly. The output of the generator is a contrastive sample of the same dimension and feature types as the input sample. To foster the generator to synthesize fake samples which are both realistic - similar to the ones in the dataset - and reflect sensitive attribute, the discriminator \( D \) is trained to perform two tasks: i) distinguishing real samples from the synthesized ones and ii) classifying real and contrastive samples w.r.t. their sensitive attribute label. The discriminator has the same architecture as in StarGAN except the convolutional layers are replaced with fully connected layers to reflect the classification task in the tabular dataset.

**Data-to-data translation: Component 1.** The objective of the conditional GAN-based model for synthesizing realistic contrastive examples can be expressed as a standard adversarial loss: \( \mathcal{L}_{adv} = \mathbb{E}_x [\log D(x)] + \mathbb{E}_{x,\bar{s}} [\log(1 - D(G(x, \bar{s})))] \). Here the generator \( G(x, \bar{s}) \) is conditioned on the input sample \( x \) and the target sensitive attribute \( \bar{s} \) and is trained to minimize the adversarial loss, whereas the discriminator aims to maximize this loss. Similarly to StarGAN, for training, we adopt the Wasserstein GAN objective [3] with gradient penalty [23]: \( \mathcal{L}_{adv} = \mathbb{E}_x [D(x)] - \mathbb{E}_{x,\bar{s}} [D(G(x, \bar{s}))] - \lambda_{cyc} \mathbb{E}_x [||\nabla_{\hat{x}} D(\hat{x})||_2 - 1]^2 \), where \( \hat{x} = \alpha x + (1 - \alpha) \bar{x} \) is sampled uniformly along a straight line between a pair of a real and a generated samples, \( \alpha \sim \mathcal{U}(0, 1) \). For tabular data, we might have categorical-valued attributes, however, we note that training a Wasserstein GAN on categorical-valued attributes is done the same way as on continuous-valued attributes [23].

**Data-to-data translation: Component 2.** To ensure that the target attribute \( \bar{s} \) is present in the synthesized sample \( \hat{x} \), an auxiliary classifier \( D_{cls} \) is introduced when optimizing both the discriminator and the generator. The classifier \( D_{cls} \) learns to predict the correct attributes of the real samples by minimizing the attribute classification loss \( \mathcal{L}_{cls}^{real} = \mathbb{E}_{x,\bar{s}} [-\log D_{cls}(x, s)] \). The generator learns to produce contrastive examples \( G(x, \bar{s}) \) with attributes \( \bar{s} \) by minimizing the corresponding classification term on contrastive examples \( \mathcal{L}_{cls}^{contrastive} = \mathbb{E}_{x,\bar{s}} [-\log D_{cls}(G(x, \bar{s}), \bar{s})] \).

**Data-to-data translation: Component 3.** When learning a translation between the domains, a cycle consistency error is applied, as in [53, 9], to preserve the content of the input through a cycle application of \( G \), \( \mathcal{L}_{cyc} = \mathbb{E}_{x,\bar{s},\bar{\bar{s}}} [||G(G(x, \bar{s}), \bar{\bar{s}}) - x||_1] \). Here the generator first synthesizes a contrastive example with the target sensitive attribute \( \bar{s} \) and then translates it back by conditioning on the attribute \( s \) of the original input sample \( x \). The \( L_1 \) norm is used as the reconstruction loss. 


Algorithm 1 Learning with contrastive examples

**Input** original data \(\{(x_n, y_n, s_n)\}_{n=1}^{N}\), contrastive examples \(\{(\bar{x}_n, \bar{s}_n)\}_{n=1}^{N}\).

Assume access to a classification algorithm that takes training data and can learn an accurate classifier \(f : \mathcal{X} \rightarrow \{0, 1\}\) (e.g. SVMs, logistic regression)

Call the algorithm with training data \(\{(x_n, y_n)\}_{n=1}^{N}\) and \(\{(\bar{x}_n, \bar{y}_n)\}_{n=1}^{N}\)

**Return** a classifier \(f^*\)

Finally, the full objective for training the generator and discriminator networks of the StarGAN model for generating contrastive examples can be written as:

\[
L_G = L_{\text{adv}} + \lambda_{\text{cls}} L_{\text{cls}}^{\text{contrastive}} + \lambda_{\text{cyc}} L_{\text{cyc}},
\]

\[
L_D = -L_{\text{adv}} + \lambda_{\text{cls}} L_{\text{cls}}^{\text{real}},
\]

where \(\lambda_{\text{cls}}\) and \(\lambda_{\text{cyc}}\) are the hyper-parameters to control relative importance of different loss terms. Note, both the discriminator and the generator are unaware of the target prediction task (e.g. predicting the income in the Adult dataset).

3 The Model

For each individual, we have a vector of non-protected features \(x \in \mathcal{X}\), a target class label \(y \in \mathcal{Y}\), and a vector of special protected features \(s \in \mathcal{S}\) (e.g. racial origin or gender). In almost all current work of fairness, \(s\) and \(y\) are assumed to be binary. It is further assumed that one of the class labels (positive label \(y = 1\)) is desirable, e.g. being accepted for a loan or being invited to an interview. *Group fairness* balances a certain condition between groups of people with different protected attributes, \(s\) versus \(\bar{s}\). The term \(\hat{y}\) below is the prediction of a machine learning model that, in most works, uses only non-protected features \(x\). Several group fairness criteria have been proposed, a popular one is called equalized odds [24, 49], which demands equality of true \(P(\hat{y} = 1|s, y = 1) = P(\hat{y} = 1|\bar{s}, y = 1)\) and false positive rates. We use this measure in our experiments.

Given the “ideal” training dataset consisting of the original and contrastive examples (Section 2), our proposed de-biasing framework is straightforward. It requires only black-box access to a standard classification algorithm (e.g. SVMs, logistic regression, multi-layer neural networks). The algorithm does not need to have any knowledge of the desired definition of fairness, and importantly, the algorithm does not use protected attributes as its input. It simply uses original examples with the corresponding target labels, and contrastive versions of the original data with the original target labels as the training dataset. Please refer to Algorithm 1 for the summary of our proposed method. The simplicity of the framework raises both advantages and concerns. Which fairness definition are we enforcing? [31] and [10] showed that most of fairness definitions are mutually exclusive except for special cases when we have a perfect predictor, or when we have a perfect dataset (the base acceptance rate is the same for both groups, i.e. true label is independent of protected attributes). We do not have perfect predictors, but we can aim to have perfect datasets. The way we create contrastive examples by intervening on protected attributes, and subsequently assigning the original target label to these contrastive examples aims to synthesize this perfect dataset. If we have a causal graph and we know that the target labels are not affected by the intervention on protected attributes, then the target labels should stay at the current observed levels. In general, applying fairness constraints in succession as “fair pipelines” do not enforce fairness [17, 7]. Our de-biasing framework relies on contrastive examples, and does not explicitly take a specific fairness definition. If desired, we could use a fairness-aware classification algorithm as part of the framework. We confirm this experimentally by using the algorithm presented in [1].
4 Experiments

To demonstrate the generality of our de-biasing framework, we apply it to tabular and image data.

**Tabular data.** The Adult Income dataset [15] is a common dataset for evaluating “fair” machine learning models. It consists of 45,222 data instances, of which we use 15,000 instances for test and the rest for training (both the StarGAN model and the de-biasing framework). The split procedure was repeated 5 times. Each instance is described in terms of 14 characteristics including gender, education, marital status, number of work hours per week among others, and the goal is to predict whether the income is larger than $50,000 or not. We transform the representation into 62 real and binary features along with the sensitive/protected attribute $s$. The features can be read from the horizontal axes in Figure 3. Following [50], we consider gender to be a protected characteristic that is only available during training. Our aim is to build models which accurately predict income without unfair bias due to gender.

**Image data.** To explore if our fairness framework transfers to data with high dimensional inputs, we consider the CelebA dataset\(^1\) [32] and the Diversity in Faces dataset (DiF)\(^2\) [34]. The CelebA dataset consists of over 200K images of celebrities, 20K of which we hold out for testing. Faces in the CelebA dataset are annotated with a variety of attributes, such as to reflect visual appearance, hair style, accessories, gender, emotional state. To simulate vision applications in which visual information is used to predict a favourable attribute (e.g., rating candidates based off a video interview), we predict the *smiling* attribute given an input image. Where as vast majority of the fairness methods have been demonstrated using a single binary sensitive attribute, our approach can naturally handle multiple sensitive attributes. We consider *male/female* and *young/old* as sensitive attributes in this dataset. Jointly they form four combinations which will correspond to four sensitive groups when classifying *smiling*. Our aim is to encourage fair predictions with respect to gender and age.

The DiF dataset has been introduced very recently and contains nearly a million human face images reflecting diversity in facial features, ethnicity, age and gender. The images are annotated with facial landmarks, craniofacial and facial symmetry features, as well as skin color information, age (both continual and discretized into seven age groups), gender. We study the effect of the skin color as a sensitive attribute related to ethnicity on the task of age classification that has been shown biased [2] previously. Specifically we perform classification into seven age groups: [0-3], [4-12], [13-19], [20-30], [31-45], [46-60], [61+], as provided with the dataset annotation. The dataset annotation contains the (estimated) individual typology angle (ITA) that could be used for representing the skin color [14]. For example, the ITA values below $-30$ correspond to dark skin color, above 55 to very light skin color. We threshold the ITA values at the dataset median (20), and use a binarized sensitive feature as skin color attribute. We report the results using 500K images for training and the remaining (nearly 412K images) for testing our model on this dataset. We discarded a small percentage of original face images due to difficulties in face detection and/or misalignment, or annotation ambiguities.

**Metrics.** Following prior work in the fairness literature [18], we focus on three important metrics for measuring model performance: overall accuracy, true positive rate (TPR) parity, and false positive rate (FPR) parity. In particular, for fair models, the TPR and FPR should be similar across different groups e.g., the TPR and FPR for predicting age should be the same across light

---

\(^1\)http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

\(^2\)https://www.research.ibm.com/artificial-intelligence/trusted-ai/diversity-in-faces/
Figure 3: Adult dataset: a batch of 50 real samples (right), their contrastives (center) and the difference between them (left). We stacked the samples for visualization purposes. Each sample has 62 features (real-valued and binary) along with the label for predicting the income and gender as a protected feature. See Section 4.1 for connections between contrastive and counterfactual examples. We also perform a two-sample test for each feature to understand whether real samples and contrastives were drawn from the same distribution or not.

Real images

GAN contrastive when intervening on gender (age unchanged)

GAN contrastive when intervening on age (gender unchanged)

GAN contrastive when intervening on both attributes gender, age

Figure 4: Examples of the original images (first row) and their GAN contrastives w.r.t. gender and age synthesized using the StarGAN model[9]. Both gender and age are binary attributes. For each real image we synthesize three contrastive examples (second, third and fourth rows).
and dark skin color. In case with multiple sensitive attributes, we perform a comparison across all groups, e.g. in CelebA we compare six TPR and FPR pairwise differences across four groups \((\text{young male}, \text{young female}, \text{old male}, \text{old female})\). By measuring the TPR and FPR differences, we can conclude if our models are fair under the equality of opportunity criteria (TPR difference should be small across groups), and equality of odds criteria (both TPR and FPR differences should be small across groups). We note that it is common for accuracy to decrease as models are more fair according to the equality of odds and equality of opportunity criteria; our goal is to build fair models while minimizing the impact on overall accuracy.

4.1 Results using tabular dataset

We visualize the contrastive examples learned on the Adult Income dataset. Figure 3 illustrates a batch of 50 datapoints stacked for visualization purposes. Figure 3 (left) shows the original samples, Figure 3 (middle) shows their contrastive examples, Figure 3 (right) shows the difference between them. The latter one allows us to analyse which features influence the attribute classifier \(D_{cls}\) to predict the opposite gender and drive the generation process of contrastive samples. The most prominent is the change in the relationship and marital status, i.e. from \(\text{Husband}\) and \(\text{Married-civ-spause}\) in real samples to \(\text{Unmarried}\) and/or \(\text{Wife}\) in contrastive samples. No changes in the workclass or education and only minor changes in occupation have been noticed. Similar conclusions hold for the whole dataset. To show this, we perform hypothesis tests using empirical maximum mean discrepancy (MMD) estimates as the test statistic \([22]\), checking whether real and contrastive features were drawn from the same distribution or not. Our results confirm that at the significance level \(\alpha = 0.01\), we can reject the null hypothesis that the two distributions are the same for all categorical-valued attributes except for workclass, education, race, and nationality.

Connections to counterfactuals. \([35, \text{Figure } 2b]\) postulate a causal graph for the Adult Income dataset. Based on this causal graph, to remove bias towards females, the direct effect of gender on income, as well as, the effect of gender on income through marital status have to be suppressed. From Figure 3 (right), and also from the two sample hypothesis testing, we can see that contrastive examples have workclass, level of education, race, and nationality variables stay at the observed levels of original data points when we intervene on gender. This means when we combine original and contrastive examples to form the “ideal dataset” for training an income classification algorithm, the classifier is able to rely on those features (remember that original and contrastive examples have the same income label). For marital status and family relationship variables, we have the exact opposite. From the viewpoint of income classifier, those variables are inconsistent (e.g. married-civ spouse has high income but also widowed given the rest of variables are unchanged), and are therefore should be ignored. This is encouraging as the causal graph also recommends suppression on the indirect effect of gender mediated by marital status. \([35]\)’s causal graph does not include categorical variables race and family relationship. From our contrastive examples, we can conclude that for gender de-biasing, we should suppress the effect of family relationship but not racial origin. We observe some difference in the continuous-valued attributes (capital gain/loss and hours per week) between contrastives and real samples. Capital gain/loss is not in the causal graph model of \([35]\). Income level has a causal connection to hours per week, however according to the graph, this connection needs to be suppressed, which has been attempted in our model.

Benchmarking on Adult Income dataset. We use logistic regression as the classification algorithm. We select the regularization parameter using 10-fold cross validation over 10 possible values \(\{500, 100, 50, 10, 5, 1, 0.5, 0.1, 0.05, 0.01\}\). To ensure that fairness cannot be achieved by sim-
Table 1: Results on the Adult Income tabular dataset. The mean and std are computed across 5 repeats. Our approach of enabling the balanced dataset with GAN-based and NN-based contrastive examples is indicated accordingly. Fair baselines are Fair Reduction [1], and Fair Reweighing [28].

| Method | Accuracy ↑ | TPR Diff. ↓ | FPR Diff. ↓ |
|--------|------------|-------------|-------------|
| Log. Reg. (real) | 85.16±0.14 | 7.98±1.52  | 7.23±0.41  |
| Fair Reweighing (real) | 84.37±0.28 | 14.30±1.16 | 1.17±0.29  |
| Log. Reg. (real and GAN) (ours) | 82.48±0.44 | 4.95±3.67  | 3.94±1.33  |
| Log. Reg. (real and NN) (ours) | 85.01±0.25 | 14.80±1.90 | 8.20±0.51  |
| Fair Reduction (real) | 83.90±0.25 | 7.56±2.93  | 5.17±0.36  |
| Fair Reduction (real and GAN) (ours) | 82.33±0.49 | 5.72±4.22  | 3.49±1.60  |
| ‡Log. Reg. (real and GAN with output consistency) (ours) | 84.04±0.42 | **4.68±6.37** | 3.33±1.99 |

‡classifier only makes a prediction if there is an agreement of outputs between original and contrastive examples (at 93% of the test samples).

By modifying regularization parameter values, the two step procedure of [16] is adopted. First, we retain the best three parameter values with highest accuracy, then the best parameter is chosen as the one with the lowest bias measure. We also compare our contrastive method with the latest fairness approach that reduces fair classification to a sequence of cost-sensitive classification problems [1]. The fairness constraint violation parameter of this reduction approach is searched over 5 values {0.005, 0.01, 0.02, 0.05, 0.1}. Table 1 shows that by augmenting the data with contrastive samples, the models consistently become more fair, as shown by lower TPR and FPR rates difference. This is true for both the logistic regression model and the Fair Reduction model.

4.2 Results using image datasets

On the CelebA dataset, we train the StarGAN model [9] conditioned on gender (male/female) and age (young/old) binary attributes using 224x224 input images for 60 epochs. On the DiF dataset, we extract and align 128x128 face crops from the dataset images and trained the model conditioned on binarized skin color (ITA attribute) for 80 epochs. Due to the DiF dataset usage restrictions, here we only illustrate contrastive examples on the CelebA dataset – see Figure 4.

**Benchmarking on CelebA dataset.** We use the ResNet50 [26] model pretrained on the large-scale facial dataset [8] as our feature extractor. We use the same evaluation set up as with the tabular datasets and report the results in Table 2. With two sensitive attributes, to rebalance the input dataset, we synthesize three contrastive examples for each input image, i.e. when intervening on gender, on age, and on both. As with the tabular datasets, we observe that training with real and contrastive examples improves fairness (equality of opportunity and equalised odds) with a limited impact on accuracy. Both, TPR and FPR differences get lower when comparing with a logistic regression classifier trained on the original dataset. We also observe similar effect with Fair Reweighing. The unique selling point for GAN contrastive is that we can actually demand our classifier to only make a prediction if outputs from original test and contrastive test examples agree. This is a form of rejection learning [12, 13]. In our setting with two protected binary attributes, this would require the prediction on a test example to agree with its three contrastive counterparts.
Table 2: Results on the CelebA HD image dataset. We report accuracy of predicting smiling using both gender (male/female; abbreviated m and f) and age (young/old; abbreviated y and o) as the two protected attributes s. Fair baseline is only Fair Reweighing [28] since Fair Reduction [1] only accepts a single binary protected attribute. TPR Diff. and FPR Diff. are a mean over six pairwise difference across four groups (using one-vs-one strategy when computing the pairwise difference).

| Method                                      | Accuracy ↑ | TPR Diff. ↓ | FPR Diff. ↓ |
|----------------------------------------------|------------|-------------|-------------|
| Log. Reg. (real)                             | 89.71      | 6.69        | 6.40        |
| Fair Reweighing (real)                       | 89.32      | **2.74**    | 3.09        |
| Log. Reg. (real and GAN) (ours)              | 88.94      | 3.50        | 2.79        |
| Log. Reg. (real and NN) (ours)               | 88.78      | 3.32        | 3.53        |
| ‡Log. Reg. (real and GAN with output consistency) (ours) | **94.15** | 3.51        | **2.18**    |

‡classifier only makes a prediction if there is an agreement of outputs between original and contrastive examples (in 17,237 out of 20,000 test examples, i.e. 86,185%).

|                      | TPR_{s=f,y} | TPR_{s=f,o} | TPR_{s=m,y} | TPR_{s=m,o} | FPR_{s=f,y} | FPR_{s=f,o} | FPR_{s=m,y} | FPR_{s=m,o} |
|----------------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Logistic Regression (real) | 94.93    | 91.47       | 85.04       | 83.69       | 20.31       | 10.37       | 10.14       | 7.58        |
| Fair Reweighing (real)   | 91.36    | 89.72       | 87.44       | 86.64       | 14.35       | 8.93        | 12.75       | 10.45       |
| Logistic Regression (real and GAN contrastive) (ours) | 90.61    | 90.91       | 85.74       | 85.54       | 15.01       | 10.54       | 13.25       | 10.33       |
| Logistic Regression (real and NN contrastive) (ours) | 91.55    | 88.06       | 87.60       | 85.07       | 12.14       | 8.40        | 14.80       | 10.14       |
| ‡Logistic Regression (real and GAN contrastive with output consistency) (ours) | 96.13    | 94.47       | 90.56       | 90.41       | 8.29        | 4.67        | 6.38        | 4.51        |

This sounds very strict, will our classifier make enough predictions on the test set? Actually, yes, it makes predictions on 17,237 test examples out of 20,000 (86,185%). With this output consistency constraint, we can achieve better performance in accuracy and fairness.

**Benchmarking on DiF dataset.** We use the same feature extractor as on CelebA and similar evaluation protocol. To rebalance the input dataset, we synthesize one contrastive examples for each input image, i.e. when intervening on skin color. We report the accuracy results of multi-class classification (where seven age groups define seven classes), and equality of opportunity (TPR Diff) and equalized odds (TPR Diff and FPR diff) results of fairness in Table 3. True positive rates difference (TPR Diff) is an average of the per-class TPR differences (TPR light versus TPR dark) across seven classes. False positive rates difference (FPR Diff) is computed similarly using per-class FPR differences. For completeness, we also report the actual TPR and FPR values, as those clearly differ across the age groups. As with all other datasets, we observe that training with real and contrastive examples improves fairness. TPR differences get lower when comparing with a logistic regression classifier trained on the original dataset. In this experiment, training
Table 3: Results on the DiF image dataset. We report accuracy of predicting seven classes that correspond to age groups: [0-3], [4-12], [13-19], [20-30], [31-45], [46-60], [61+]. We use skin color (light/dark; abbreviated l and d) as the protected attribute s. Fair baseline is Fair Reweighing [28]. TPR Diff is an average of the per class TPR differences (TPR light versus TPR dark) across seven classes (age groups). FPR Diff is computed similarly.

| Method | Accuracy ↑ | TPR Diff. ↓ | FPR Diff. ↓ |
|--------|------------|-------------|-------------|
| Log. Reg. (real)                  | 69.79  | 1.55        | 0.76        |
| Fair Reweighing (real)            | 69.79  | 0.98        | 0.52        |
| Log. Reg. (real and GAN) (ours)   | 69.83  | 1.13        | 0.64        |
| Log. Reg. (real and NN)(ours)     | 69.72  | 1.43        | 0.63        |
| ‡Log. Reg. (real and GAN with output consistency) (ours) | 72.26  | 0.68        | 0.27        |

‡classifier only makes a prediction if there is an agreement of outputs (in 361674 out of 412556 test examples, i.e. 87.67%).

| [0-3] | [4-12] | [13-19] | [20-30] | [31-45] | [46-60] | [61+] |
|-------|--------|--------|--------|--------|--------|-------|
| TPR_d | TPR_l  | TPR_d  | TPR_l  | TPR_d  | TPR_l  | TPR_d |
| 87.35 | 88.77  | 85.83  | 85.77  | 14.62  | 15.28  | 69.32 |
| Fair Reweighing (real)            | 87.69  | 88.62  | 85.55  | 85.92  | 14.36  | 15.56  | 70.32 |
| Logistic Regression (real and GAN contrastive) (ours) | 87.84  | 89.11  | 86.43  | 86.42  | 15.79  | 16.52  | 69.59 |
| Logistic Regression (real and NN contrastive) (ours) | 83.18  | 85.03  | 86.44  | 87.12  | 18.39  | 19.69  | 69.82 |
| ‡Logistic Regression (real and GAN contrastive with output consistency) (ours) | 90.04  | 89.93  | 89.16  | 89.41  | 10.02  | 9.96   | 73.86 |

| [0-3] | [4-12] | [13-19] | [20-30] | [31-45] | [46-60] | [61+] |
|-------|--------|--------|--------|--------|--------|-------|
| FPR_d | FPR_l  | FPR_d  | FPR_l  | FPR_d  | FPR_l  | FPR_d |
| 0.72  | 0.97   | 2.08   | 2.16   | 0.65   | 0.58   | 14.04 |
| Fair Reweighing (real)            | 0.74   | 0.96   | 2.05   | 2.18   | 0.63   | 0.60   | 14.46 |
| Logistic Regression (real and GAN contrastive) (ours) | 0.73   | 0.97   | 2.14   | 2.22   | 0.68   | 0.63   | 14.08 |
| Logistic Regression (real and NN contrastive) (ours) | 0.49   | 0.69   | 2.19   | 2.30   | 0.91   | 0.85   | 14.28 |
| ‡Logistic Regression (real and GAN contrastive with output consistency) (ours) | 0.70   | 0.79   | 1.85   | 1.90   | 0.30   | 0.27   | 13.84 |

with contrastive examples also slightly improves recognition accuracy. This can be seen from the improvement in TPR values in the groups [4-12], [13-19] and [61+]. Fair Reweighing also helps to lower the TPR and FPR differences. With the output consistency constraint, we can achieve the best performance in terms of accuracy 72.26% and fairness (0.68 and 0.27 TPR and FPR
differences) with an agreement rate 87.67%. Overall, the fairness metric has low discrepancy w.r.t. skin color on this dataset, supporting its main purpose of collecting many diverse face images. Nevertheless, the proposed approach can improve over the baselines.

Visualizing Important Visual Attributes for Classification. By producing contrastive examples in the input space, we can qualitatively evaluate what our models focus on during prediction for our test images. To visualize which visual attributes are important for our models, we rely on Grad-CAM [42] which traces gradients to determine which locations in an image are most important for a decision. Figure 5 shows visualizations for a model trained on real images and a model trained on real and contrastive images, controlling for gender and age as the protected characteristic. When classifying images, the models tend to focus not only on the mouth area, but also on the center of the face, with important regions including the nose and forehead. The Grad-CAM visualizations show that the model trained on both real and contrastive images, is more localized on the mouth area of the face, which is an expected behavior for classifying smiling. We noticed such differences were more pronounced in pictures of males rather than females. This is also expected as the male group suffers higher classification error for this task. Also we note that the model trained with contrastive images consistently predicts the correct class (smiling), suggesting that the model has learned to better “ignore” gender and age when making a prediction.

5 Discussions and Conclusion

GANs are not just good for causing mischief.
Karen Hao, MIT Technology Review

In this work we present an intuitive method to train fair AI systems: instead of relying only on the original training data, we intervene on training instances and generate contrastive examples. By simply building a more “ideal” training dataset, trained models become more fair and less susceptible to uncertainty bias for a variety of input types (tabular data and natural images). To generate contrastive examples, we build upon progress in image generation. We demonstrate that current GAN frameworks can easily be extended to very different input modalities (e.g., tabular data), and that contrastive examples provide a means to interpret fair models. As shown on the Adult Income dataset, our contrastive examples are closely related to counterfactuals. AI is becoming more and more ubiquitous, and it is imperative that our learning systems can be fair and interpretable. We believe integrating contrastive reasoning via generative models is an important step towards this goal. In short, generative models are not just good at causing mischief, but can be a key component in building fair AI systems.
Acknowledgements

VS is supported by the Imperial College Research Fellowship. NQ is supported by the European Research Council (ERC) funding, grant agreement No 851538. We gratefully acknowledge NVIDIA for GPUs donation and Amazon for AWS Cloud Credits.

References

[1] Alekh Agarwal, Alina Beygelzimer, Miroslav Dudík, John Langford, and Hanna Wallach. A reductions approach to fair classification. In International Conference on Machine Learning (ICML), volume 80 of Proceedings of Machine Learning Research, pages 60–69, 2018. 2, 6, 10, 11

[2] Mohsan Alvi, Andrew Zisserman, and Christoffer Nellåker. Turning a blind eye: Explicit removal of biases and variation from deep neural network embeddings. In Proceedings of the European Conference on Computer Vision (ECCV), pages 0–0, 2018. 3, 7

[3] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In International Conference on Machine Learning, 2017. 5

[4] Solon Barocas, Kate Crawford, Aaron Shapiro, and Hanna Wallach. The problem with bias: from allocative to representational harms in machine learning. In Special Interest Group for Computing, Information and Society (SIGCIS), 2017. 2

[5] S. Barocas and A. Selbst. Big data’s disparate impact. California Law Review, 104(3):671–732, 2016. 3

[6] Alex Beutel, Jilin Chen, Zhe Zhao, and Ed H. Chi. Data decisions and theoretical implications when adversarially learning fair representations. CoRR, abs/1707.00075, 2017. 2

[7] Amanda Bower, Sarah N. Kitchen, Laura Niss, Martin J. Strauss, Alexander Vargas, and Suresh Venkatasubramanian. Fair pipelines. CoRR, abs/1707.00391, 2017. 6

[8] Qiong Cao, Li Shen, Weidi Xie, Omkar M Parkhi, and Andrew Zisserman. VGGFace2: A dataset for recognising faces across pose and age. In Automatic Face & Gesture Recognition (FG 2018), pages 67–74, 2018. 10

[9] Yunjey Choi, Minje Choi, Munyoung Kim, Jung-Woo Ha, Sunghun Kim, and Jaegul Choo. Stargan: Unified generative adversarial networks for multi-domain image-to-image translation. In IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018. 5, 8, 10

[10] Alexandra Chouldechova. Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. Big data, 5(2):153–163, 2017. 4, 6

[11] Alexandra Chouldechova and Aaron Roth. The frontiers of fairness in machine learning. CoRR, abs/1810.08810, 2018. 1

[12] C. K. Chow. An optimum character recognition system using decision functions. IRE Transactions on Electronic Computers, EC-6(4):247–254, 1957. 2, 10

[13] Corinna Cortes, Giulia DeSalvo, and Mehryar Mohri. Learning with rejection. In International Conference on Algorithmic Learning Theory (ALT), 2016. 2, 10

[14] Sandra Del Bino and F Bernerd. Variations in skin colour and the biological consequences of ultraviolet radiation exposure. British Journal of Dermatology, 169:33–40, 2013. 7

[15] Dua Dheeru and Efi Karra Taniskidou. UCI machine learning repository, 2017. 5, 7

[16] Michele Donini, Luca Oneto, Shai Ben-David, John S Shawe-Taylor, and Massimiliano Pontil. Empirical risk minimization under fairness constraints. In Advances in Neural Information Processing Systems (NeurIPS), pages 2796–2806, 2018. 10

[17] Cynthia Dwork and Christina Ilvento. Fairness under composition. CoRR, abs/1806.06122, 2018. 6

[18] Sorelle A Friedler, Carlos Scheidegger, Suresh Venkatasubramanian, Sonam Choudhary, Evan P Hamilton, and Derek Roth. A comparative study of fairness-enhancing interventions in machine learning. arXiv preprint arXiv:1802.04422, 2018. 7
[19] Yaroslav Ganin, Evgeniya Ustinova, Hana Ajakan, Pascal Germain, Hugo Larochelle, François Laviolette, Mario Marchand, and Victor Lempitsky. Domain-adversarial training of neural networks. *Journal of Machine Learning Research (JMLR)*, 17:2096–2030, 2016. 3

[20] Clare Garvie. *The perpetual line-up: Unregulated police face recognition in america*. Georgetown Law, Center on Privacy & Technology, 2016. 2

[21] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 2672–2680, 2014. 2

[22] Arthur Gretton, Karsten M. Borgwardt, Malte J. Rasch, Bernhard Schölkopf, and Alexander J. Smola. A kernel two-sample test. *Journal of Machine Learning Research*, 13:723–773, 2012. 9

[23] Ishaan Gulrajani, Faruk Ahmed, Martín Arjovsky, Vincent Dumoulin, and Aaron C. Courville. Improved training of Wasserstein GANs. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2017. 5

[24] Moritz Hardt, Eric Price, and Nati Srebro. Equality of opportunity in supervised learning. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 3315–3323, 2016. 3, 6

[25] Tatsunori Hashimoto, Megha Srivastava, Hongseok Namkoong, and Percy Liang. Fairness without demographics in repeated loss minimization. In *Proceedings of the 35th International Conference on Machine Learning*, volume 80 of *Proceedings of Machine Learning Research*, pages 1929–1938. PMLR, 2018. 1

[26] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016. 10

[27] Judy Hoffman, Eric Tzeng, Taesung Park, Jun-Yan Zhu, Phillip Isola, Kate Saenko, Alexei A Efros, and Trevor Darrell. Cycada: Cycle-consistent adversarial domain adaptation. *arXiv preprint arXiv:1711.03213*, 2017. 3

[28] F. Kamiran and T. Calders. Data preprocessing techniques for classification without discrimination. *Knowledge and Information Systems*, 33(1):1–33, 2012. 2, 10, 11, 12

[29] Toshihiro Kamishima, Shotaro Akaho, Hideki Asoh, and Jun Sakuma. Fairness-aware classifier with prejudice remover regularizer. In *European conference on Machine Learning and Knowledge Discovery in Databases (ECML PKDD)*, pages 35–50, 2012. 3

[30] Jinkyu Kim and John Canny. Interpretable learning for self-driving cars by visualizing causal attention. In *IEEE International Conference on Computer Vision (ICCV)*, pages 2961–2969, 2017. 3

[31] Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan. Inherent trade-offs in the fair determination of risk scores. In *Innovations in Theoretical Computer Science Conference (ITCS)*, 2017. 4, 6

[32] Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. Deep learning face attributes in the wild. In *Proceedings of International Conference on Computer Vision (ICCV)*, 2015. 7

[33] David Madras, Elliot Creager, Toniann Pitassi, and Richard S. Zemel. Learning adversarially fair and transferable representations. *CoRR*, abs/1802.06309, 2018. 2

[34] Michele Merler, Nalini K. Ratha, Rogério Schmidt Feris, and John R. Smith. Diversity in faces. *CoRR*, abs/1901.10436, 2019. 3, 7

[35] Razieh Nabi and Ilya Shpitser. Fair inference on outcomes. In *Association for the Advancement of Artificial Intelligence (AAAI)*, pages 1931–1940, 2018. 9

[36] Vitali Petsiuk, Abir Das, and Kate Saenko. Rise: Randomized input sampling for explanation of black-box models. *arXiv preprint arXiv:1806.07421*, 2018. 3

[37] Novi Quadrianto and Viktoriia Sharmanska. Recycling privileged learning and distribution matching for fairness. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2017. 3

[38] Novi Quadrianto, Viktoriia Sharmanska, and Oliver Thomas. Discovering fair representations in the data domain. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019. 3
[39] Paul R. Rosenbaum and Donald B. Rubin. The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70(1):41–55, 1983. 2

[40] Hee Jung Ryu, Hartwig Adam, and Margaret Mitchell. InclusiveFaceNet: Improving face attribute detection with race and gender diversity. In *FATML workshop*, 2017. 3

[41] Prasanna Sattigeri, Samuel C. Hoffman, Vijil Chenthamarakshan, and Kush R. Varshney. Fairness GAN. *arXiv*, arXiv:1805.09910, 2018. 3

[42] Ramprasaath R Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *2017 IEEE International Conference on Computer Vision (ICCV)*, pages 618–626, 2017. 13

[43] Ashish Shrivastava, Tomas Pfister, Oncel Tuzel, Joshua Susskind, Wenda Wang, and Russell Webb. Learning from simulated and unsupervised images through adversarial training. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 2242–2251, 2017. 3

[44] Eric Tzeng, Judy Hoffman, Trevor Darrell, and Kate Saenko. Simultaneous deep transfer across domains and tasks. In *International Conference on Computer Vision (ICCV)*, pages 4068–4076, 2015. 3

[45] Mark J. van der Laan and Sherri Rose. *Targeted Learning: Causal Inference for Observational and Experimental Data*. Springer, 2011. 4

[46] Sandra Wachter, Brent Mittelstadt, and Chris Russell. Counterfactual explanations without opening the black box: Automated decisions and the gdpr. *Harvard Journal of Law and Technology*, 31:841–887, 2018. 3

[47] Mei Wang, Weihong Deng, Jiani Hu, Xunqiang Tao, and Yaohai Huang. Racial faces in the wild: Reducing racial bias by information maximization adaptation network. In *International Conference on Computer Vision (ICCV)*, pages 692–702, 2019. 3

[48] Qizhe Xie, Zihang Dai, Yulun Du, Eduard Hovy, and Graham Neubig. Controllable invariance through adversarial feature learning. In *Advances in Neural Information Processing Systems (NeurIPS)*, pages 585–596, 2017. 2

[49] Muhammad Bilal Zafar, Isabel Valera, Manuel Gomez-Rodriguez, and Krishna P. Gummadi. Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment. In *International Conference on World Wide Web (WWW)*, pages 1171–1180, 2017. 3, 6

[50] Richard Zemel, Yu Wu, Kevin Swersky, Toniann Pitassi, and Cynthia Dwork. Learning fair representations. In *International Conference on Machine Learning (ICML)*, Proceedings of Machine Learning Research, pages 325–333. PMLR, 2013. 2, 7

[51] Brian Hu Zhang, Blake Lemoine, and Margaret Mitchell. Mitigating unwanted biases with adversarial learning. In *Association for the Advancement of Artificial Intelligence (AAAI)*, 2018. 2

[52] Zhifei Zhang, Yang Song, and Hairong Qi. Age progression/regression by conditional adversarial autoencoder. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 5810–5818, 2017. 3

[53] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A Efros. Unpaired image-to-image translation using cycle-consistent adversarial networks. In *International Conference on Computer Vision (ICCV)*, 2017. 5