Adversarial Learning for Counterfactual Fairness

Vincent Grari  
Sorbonne Université LIP6/CNRS  
Paris, France  
vincen.grari@lip6.fr

Sylvain Lamprier  
Sorbonne Université LIP6/CNRS  
Paris, France  
sylvain.lamprier@lip6.fr

Marcin Dety nieck i  
AXA REV Research  
Paris, France  
marcin.detyniecki@axa.com

Abstract—In recent years, fairness has become an important topic in the machine learning research community. In particular, counterfactual fairness aims at building prediction models which ensure fairness at the most individual level. Rather than globally considering equity over the entire population, the idea is to imagine what any individual would look like with a variation of a given attribute of interest, such as a different gender or race for instance. Existing approaches rely on Variational Auto-encoding of individuals, using Maximum Mean Discrepancy (MMD) penalization to limit the statistical dependence of inferred representations with their corresponding sensitive attributes. This enables the simulation of counterfactual samples used for training the target fair model, the goal being to produce similar outcomes for every alternate version of any individual. In this work, we propose to rely on an adversarial neural learning approach, that enables more powerful inference than with MMD penalities, and is particularly better fitted for the continuous setting, where values of sensitive attributes cannot be exhaustively enumerated. Experiments show significant improvements in term of counterfactual fairness for both the discrete and the continuous settings.

Index Terms—Counterfactual Fairness, Adversarial Neural Network, Causal Inference

I. INTRODUCTION

Machine learning models have an increasingly important role in our daily lives and can have significant implications for citizens like loan applications, recidivism score, credit rating, etc. However, the data used for training the models can reflect sensitive biases that exist in our society and without a careful design the models can perpetuate or even reinforce these biases [1]. Many incidents of this kind have been reported in recent years. An infamous example is the case of a tool for criminal risk prediction (COMPAS), which showed strong discrimination against black defendants [2].

A fair predictive model provides outcomes that do not contain any prejudice or favoritism toward an individual or a group based on a set of sensitive characteristics. One of the problems in achieving a non-discriminatory model is that it is not simply a matter of removing protected attributes from the training base [3]. This concept, known as "fairness through unawareness," is highly insufficient because any other non-sensitive attribute might indirectly contain significant sensitive information. To tackle this problem the recent fair machine learning research field has emerged.

As of now, a large majority of works in the field focused on group fairness metrics, that assess a form of conditional independence between the 3 following features: the sensitive attribute $A$, the true outcome feature $Y$, and the output model predictions $\hat{Y}$. For example, one of the most known objective Demographic parity ensures that the output prediction is not dependent of the sensitive feature $A$ [4, 5]. However, predictive models trained to be fair regarding such group metrics may induce dramatic consequences for some individuals. For example in an extreme case, a person may be refused a position only because of belonging to a privileged group, regardless of their merit within the group. To tackle such issues, a recent field called Counterfactual fairness [6] recently proposed to assess fairness at the individual level, by leveraging causal inference to ensure that some sensitive attributes are not the cause of a prediction change. It argues to lead to a more intuitive, powerful, and less error-prone way of reasoning about fairness [7]. The idea is to imagine what any individual would look like with a variation of a given attribute of interest, such as a different gender or race for instances, in order to ensure similar outcomes for every alternate version of the same individual. While plenty of methods have been proposed recently to tackle this challenge for discrete variables, to the best of our knowledge no approach address the continuous case. The existing approches may not hold when, for instance, the sensitive attribute is the age or the weight of an individual.

The main contributions of this paper are:

- We propose an adversarial approach for confounding variable inference, which allows the generation of accurate counterfactuals in both discrete and continuous sensitive settings (while existing approaches are limited to the discrete case);
- Based on this, we define an approach for counterfactual fairness tolerant to continuous features, notably via a dynamic sampling method that focuses on individualized hard locations of the sensitive space;
- We demonstrate empirically that our algorithm can mitigate counterfactual fairness

Section 2 first gives details for counterfactual fairness, which we believe are essential for a good understanding of our contributions. Then, in section III we detail our approach in two main steps. Section IV evaluates performances for both the discrete and the continuous settings.
II. BACKGROUND

Recently, there has been a dramatic rise of interest for fair machine learning by the academic community. Many questions have been raised, such as: How to define fairness [6, 8, 9, 10]? How to mitigate the sensitive bias [5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]? How to keep a high prediction accuracy while remaining fair in a complex real-world scenario [21, 22] ? To answer these questions, three main families of fairness approaches exist in the literature. While pre-processing [13, 14, 15] and post-processing [9, 19] approaches respectively act on the input or the output of a classically trained predictor, pre-processing [13, 14, 15] and post-processing [9, 19] approaches respectively act on the input or the output of a classically trained predictor, in-processing approaches mitigate the undesired bias directly during the training phase [5, 11, 15, 17, 18]. In this paper we focus on in-processing fairness, which reveals as the most powerful framework for settings where acting on the training process is an option.

Throughout this document, the aim is to learn a predictive function \( h_\theta \) from training data that consists of \( m \) examples \( (x_i, a_i, y_i)_{i=1}^m \), where \( x_i \in \mathbb{R}^p \) is the \( p \)-sized feature vector \( X \) of the \( i \)-th example, \( a_i \in \Omega_A \) the value of its sensitive attribute and \( y_i \) its label to be predicted. According to the setting, the domain \( \Omega_A \) of the sensitive attribute \( A \) can be either a discrete or a continuous set. The outcome \( Y \) is also either binary or continuous. The objective is to ensure some individual fairness guarantees on the outcomes of the predictor \( \hat{Y} = h_\theta(X, A) \), by the way of Counterfactual Fairness. The remaining of this section presents classical and Counterfactual Fairness Metrics and existing methods for Counterfactual Fairness.

A. Fairness definitions and metrics

The vast majority of fairness research works have focused on two metrics that have become very popular in the fairness field: Demographic parity [10] and Equalized odds [9]. Both of them consider fairness globally, by focusing on equity between groups of people, defined according to one or several high level sensitive attributes. The Demographic parity metric compares the average prediction for each demographic sensitive group. For instance, in the binary discrete case, it comes down to ensure that: \( P(\hat{Y} = 1|A = 0) = P(\hat{Y} = 1|A = 1) \). The underlying idea is that each sensitive demographic group must own the same chance for a positive outcome. The Equalized odds metric rather compares rates of True positives and False positives between sensitive groups: \( P(\hat{Y} = 1|A = 0, Y = y) = P(\hat{Y} = 1|A = 1, Y = y) \), \( \forall y \in \{0, 1\} \). The notion of fairness here is that chances for being correctly or incorrectly classified as positive should be equal for every group. However, these metrics which correspond to averages over each sensitive groups are known to lead to arbitrary individual-level fairness deviations, with a high outcome variance within groups [20].

In the continuous setting, some recent works proposed to consider non-linear correlation metrics between the predicted outcome \( \hat{Y} \) and the sensitive attribute \( A \), such as the Hirschfeld-Gebelein-Rényi maximal correlation (HGR) defined, for two jointly distributed random variables \( U \in \mathcal{U} \) and \( V \in \mathcal{V} \), as:

\[
\text{HGR}(U, V) = \sup_{f: \mathcal{U} \rightarrow \mathcal{U}, g: \mathcal{V} \rightarrow \mathcal{V}} \rho(f(U), g(V))
\]

where \( \rho \) is the Pearson linear correlation coefficient with some measurable functions \( f \) and \( g \). The HGR coefficient is equal to 0 if the two random variables are independent. If they are strictly dependent the value is 1. Applied to fairness [12, 23, 24], it can be used to measure objectives similar to those defined for the discrete setting, such as the Demographic parity, which can be measured via \( \text{HGR}(\hat{Y}, A) \) (this accounts for the violation level of the constraint \( P(\hat{Y}|A) = P(\hat{Y}) \)).

However, even such approaches in the continuous setting only consider fairness globally and can lead to particularly unfair decisions at the individual level. For example, a fair algorithm can choose to accept a high MSE error for the outcome of a given person if this allows the distribution \( P(\hat{Y}|A) \) to get closer to \( P(\hat{Y}) \). Penalization can be arbitrarily high on a given kind of individual profile compared to any other equivalent one, only depending on where the learning process converged. Global fairness is unfair.

To tackle this problem, Counterfactual fairness has been recently introduced for quantifying fairness at the most individual sense [6]. The idea is to consider that a decision is fair for an individual if it coincides with the one that would have been taken in a counterfactual world in which the values of its sensitive attributes were different. It leverages the previous work [24], which introduced a causal framework to learn from biased data by exploring the relationship between sensitive features and data. With the recent development in deep learning, some novels approaches [25, 26, 27] argue to lead to a less error-prone decision-making model, by improving the approximation of the causal inference in the presence of unobserved confounders.

**Definition 1:** Counterfactual demographic parity [6]: A predictive function \( h_\theta \) is considered counterfactually fair for a causal world \( G \), if for any \( x \in \mathcal{X} \) and \( \forall y \in \mathcal{Y}, \forall (a, a') \in \Omega_A^2 \) with \( a \neq a' \):

\[
p(\hat{Y}_{A \leftarrow a} = y|X = x, A = a) = p(\hat{Y}_{A \leftarrow a'} = y|X = x, A = a)
\]

where \( \hat{Y}_{A \leftarrow a'} = h_\theta(\hat{X}_{A \leftarrow a'}) \) is the outcome of the predictive function \( h_\theta \) for any transformation \( \hat{X}_{A \leftarrow a'} \) of input \( X \), resulting from setting \( a' \) as its sensitive attribute value, according to the causal graph \( G \).

Following definition [6] an algorithm is considered counterfactually fair in term of demographic parity if the predictions are equal for each individual in the factual causal world where \( A = a \) and in any counterfactual world where \( A = a' \). It therefore compares the predictions of the same individual with an alternate version of him/herself. Similar extension can be done to adapt the Equalized Odds objective for the Counterfactual framework [26]. Learning transformations \( \hat{X}_{A \leftarrow a'} \) for
a given causal graph is at the heart of Counterfactual Fairness, as described in the next subsection.

B. Counterfactual Fairness

In this paper, we focus on the classical causal graph depicted in Fig.1, often used in the counterfactual fairness literature [6 7 26], which can apply for most applications. For more specific tasks, note further that our approach could be easily adapted for different graphs, such as those explored in [6] for instances. In this causal graph, both input X and outcome Y only depend on the sensitive attribute A and a latent variable U, which represents all the relevant knowledge non dependent on the sensitive feature A. In that setting, the knowledge of U can be used during training to simulate various versions of the same individual, corresponding to different values of A, in order to obtain a predictive function hθ which respects the fairness objective from definition 1. For any training individual, U has to be inferred since only X, A and Y are observed. This inference must however ensure that no dependence is created between U and A (no arrow from U to A in the graph from Fig.1), unless preventing the generation of proper alternative versions of X and Y for any values A.

A classic way to achieve a counterfactually fair model is to proceed with two distinct main steps of Causal Inference and Model Learning [26 28], that are described below.

1) Step 1: Counterfactual Inference: The goal is to define a way to generate counterfactual versions of original individuals. As discussed above, this is usually done via approximate Bayesian inference, according to a pre-defined causal graph.

The initial idea to perform inference was to suppose with strong hypothesis a non deterministic structural model with some specific distribution for all the causal links [6]. In this setting, the posterior distribution of U was estimated using the probabilistic programming language Stan [29]. Then, leveraging recent developments for approximate inference with deep learning, many works [7 25 26 27] proposed to use Variational Autoencoding [30] methods (VAE) to generalize this first model and capture more complex - non linear - dependencies in the causal graph.

Following the formulation of VAE, it would be possible to directly optimize the classical lower bound (ELBO) [30] on the training set D, by minimizing:

\[
\mathcal{L}_{ELBO} = - \mathbb{E}_{(x,y,a) \sim D} \left[ \log p_0(x, y|u, a) \right] + D_{KL}(q_\phi(u|x, y, a)||p(u))
\]

where \(D_{KL}\) denotes the Kullback-Leibler divergence of the posterior \(q_\phi(u|x, y, a)\) from a prior \(p(u)\), typically a standard Gaussian distribution \(\mathcal{N}(0, I)\). The posterior \(q_\phi(u|x, y, a)\) is represented by a deep neural network with parameters \(\phi\), which typically outputs the mean \(\mu_\phi\) and the variance \(\sigma_\phi\) of a diagonal Gaussian distribution \(\mathcal{N}(\mu_\phi, \sigma_\phi I)\). The likelihood term factorizes as \(p_0(x, y|u, a) = p_0(x|u, a)p_0(y|u, a)\), which are defined as neural networks with parameters \(\theta\). Since attracted by a standard prior, the posterior is supposed to remove probability mass for any features of the latent representation U that are not involved in the reconstruction of X and Y. Since A is given together with U as input of the likelihoods, all the information from A should be removed from the posterior distribution of U.

However, many state of the art algorithms [7 25 26 27] show that the independence level between the latent space U and the sensitive variable A is insufficient with this classical ELBO optimization. Some information from A leaks in the inferred U. In order to ensure a high level of independence, a specific TARNet [31] architecture can be employed [25] or a penalisation term can be added in the loss function. For example, [7 26] add a Maximum Mean Discrepancy (MMD) [32] constraint. The MMD term can be used to enforce all the different aggregated posterior to the prior distribution [26]:

\[
\mathcal{L}_{MMD}(q_\phi(u|A = a_k)||p(u)) \quad \text{for all} \quad a_k \in \Omega_A
\]

(2)

(2)

Alternatively, the constraint can directly enforce the matching between pairs of posteriors [7]:

\[
\mathcal{L}_{MMD}(q_\phi(u|A = a_k)||q_\phi(u|A = a)) \quad \text{for all} \quad a_k \in \Omega_A,
\]

with \(a\) standing for the original sensitive value of the considered individual (referred to as MMD wrt \(U_a\) in the following). Notice that while this additional term can improve independence, it can also encourage the model to ignore the latent confounders U, by being too restrictive. One possible approach to address this issue is to apply weights \(\lambda\) (hyperparameters) to control the relative importance of the different terms. In addition, we employ in this paper a variant of the ELBO optimization as done in [26], where the \(D_{KL}(q_\phi(u|x, y, a)||p(u))\) term is replaced by a MMD term \(\mathcal{L}_{MMD}(q_\phi(u)||p(u))\) between the aggregated posterior \(q_\phi(u)\) and the prior. This has been shown more powerful than the classical \(D_{KL}\) for ELBO optimization in [33], as the latter can reveal as too restrictive (uninformative latent code problem) [34 35 36] and can also tend to overfit the data (Variance Over-estimation in Feature Space). Finally, the inference for
Counterfactual fairness can be optimized by minimizing [26]:

$$L_{CE-VAE} = - \mathbb{E}_{(x,y,a) \sim D, \ U \sim p(U|X,Y,A)} \left[ \lambda_x \log(p_{\theta}(x|u,a)) + \lambda_y \log(p_{\theta}(y|u,a)) \right] + \lambda_{MMD} \text{MMD}(q_{\phi}(u)||p(u)) + \lambda_{ADV} \frac{1}{m_a} \sum_{a \in \Omega_A} \text{MMD}(q_{\phi}(u|a = a_k)||p(u))$$

where $\lambda_x, \lambda_y, \lambda_{MMD}, \lambda_{ADV}$ are scalar hyperparameters and $m_a = |\Omega_A|$. The additional MMD objective can be interpreted as minimizing the distance between all moments of each aggregated latent code distribution and the prior distribution, in order to remove most sensitive dependency from the code generator. It requires however a careful design of the kernel used for MMD computations (typically a zero mean isotropic Gaussian). Note that we chose to present all models with a generic inference scheme $q(U|X,Y,A)$, while most approaches from the literature only consider $q(U|X,A)$. The use of $Y$ as input is allowed since $U$ is only used during training, for generating counterfactual samples used to learn the predictive model in step 2. Various schemes of inference are considered in our experiments (section IV).

2) Step 2: Counterfactual predictive model: Once the causal model is learned, the goal is to use it to learn a fair predictive function $h_{\theta}$, by leveraging the ability of the model to generate alternative versions of each training individual. The global loss function is usually composed of the traditional predictor loss $l(h_{\theta}(x_i, a_i), y_i)$ (e.g. cross-entropy for instance $i$) and the counterfactual unfairness estimation term $L_{CF}(\theta)$:

$$L = \frac{1}{m} \sum_{i=1}^{m} l(h_{\theta}(x_i), y_i) + \lambda L_{CF}(\theta)$$

where $\lambda$ is an hyperparameter which controls the impact of the counterfactual loss in the optimization. The counterfactual loss $L_{CF}(\theta)$ considers differences of predictions for alternative versions of any individual. For example, [28] considers the following Monte-Carlo estimate from $S$ samples for each individual $i$ and each value $a \in \Omega_A$:

$$L_{CF}(\theta) = \frac{1}{m} \sum_{i=1}^{m} \frac{1}{m_a} \sum_{a \in \Omega_A} \frac{1}{S} \sum_{s=1}^{S} \Delta_{a_k}^{i,a}$$

where $\Delta_{a_k}^{i,a} = \Delta(h_{\theta}(x_i^{s,a}, A_{i-a_1}, a_1), h_{\theta}(x_i^{s,a}, A_{i-a_1}, a_k))$ is a loss function that compares two predictions, $x_i^{s,a}$ denotes the $s$-th sample from the causal model for the $i$-th individual of the training set and the sensitive attribute value $a$. Following the causal model learned at step 1, $x_i^{s,a}$ is obtained by first inferring a sample $u$ from $q_{\phi}(u|x_i, a_1, y_i)$ and then sampling $x_i^{s,a}$ using $p_{\theta}(x|u,a)$ with the counterfactual (or factual) attribute value $a$. According to the task, $\Delta$ can take various forms. For binary classification, it can correspond to a logit paring loss as done in [29]: $\Delta(z, z') = \sigma^{-1}(z) - \sigma^{-1}(z')^2$, where $\sigma^{-1}$ is the logit function. For continuous outcomes, it can simply correspond to a mean squared difference.

3) Discussion: For now, state-of-the-art approaches have focused specifically on categorical variables $A$. Unfortunately, the classical methodology for CounterFactual Fairness as described above cannot be directly generalized for continuous sensitive attributes, because the two steps involve enumerations of the discrete counterfactual modalities $a_k$ in the set $\Omega_A$. Particularly in step 1, sampling $A$ from a uniform distribution for approximating the expectation $E_{a \sim p(A)} \text{MMD}(q_{\phi}(u|A = a)||p(u))$ is not an option since this requires to own a good estimation of $q_{\phi}(u|A = a)$ for any $a \in \Omega_A$, which is difficult in the continuous case. While such a posterior can be obtained for discrete sensitive attributes (at least when $|\Omega_A| << m$) by aggregating the posteriors $q_{\phi}(u|x_i, a_i, y_i)$ over training samples $i$ such that $a_i = a$, such a simple aggregation over filtered samples is not possible for continuous attributes. Moreover, existing approaches based on MMD costs imply to infer codes $U$ from a distribution that takes $A$ as input, in order to be able to obtain the required aggregated distributions via: $q_{\phi}(u|a) = \mathbb{E}_{p_{x, y, a}}[q_{\phi}(u|x, y, a)]$. Omitting $A$ from the conditioning of the generator would correspond to assume the mutual independence of $u$ and $a$ given $x$ and $y$, which is usually wrong. On the other hand, passing $A$ to the generator of $U$ can encourage their mutual dependency in some settings, as we observe in our experiments.

III. ADVERSARIAL LEARNING FOR COUNTERFACTUAL FAIRNESS

In this section we revisit the 2 steps shown above by using adversarial learning rather than MMD costs for ensuring Counterfactual Fairness. Our contribution covers a broad range of scenarios, where the sensitive attribute $A$ and the outcome value $Y$ can be either discrete or continuous.

Figure 2: Architecture of our Counterfactual inference process. Blue arrows represent the retro-propagated gradients for the minimization of the global objective. The red one corresponds to the gradients for the adversarial optimization. Circles are observed variables, squares are samples from the neural distributions.

1) Step 1: Counterfactual Inference: To avoid the comparison of distributions for each possible sensitive value, which
reveals particularly problematic in the continuous setting, we propose to employ an adversarial learning framework, which allows one to avoid the enumeration of possible values in $\Omega_A$. We follow an approach similar to the adversarial auto-encoders proposed in [37], but where the discriminator real/fake data is replaced by a sensitive value predictor. The idea is to avoid any adversarial function to be able to decode $A$ from the code $U$ inferred from the encoder $q_\psi$, which allows one to ensure mutual independence of $A$ and $U$. This defines a two-players adversarial game, such as in GANs [38], where the goal is to find some parameters $\phi$ which minimize the loss to reconstruct $X$ and $Y$, while maximizing the reconstruction loss of $A$ according to the best decoder $p_\psi(A|U)$:

$$\arg\min_{\theta,\phi} \max_{\psi} L_{ADV}(\theta, \phi, \psi)$$

with, for the graphical causal model from figure 1

$$L_{ADV}(\theta, \phi, \psi) = - \mathbb{E}_{(x,y,a) \sim D, \ u \sim q_\psi(u|x, y, a)} \left[ \lambda_x \log(p_\theta(x|u, a)) + \lambda_y \log(p_\theta(y|u, a)) \right]$$

$$+ \lambda_{MMD} \mathcal{L}_{MMD}(q_\psi(u)) \| p(u) \|$$

$$+ \lambda_{ADV} \mathbb{E}_{(x,a) \sim D, \ u \sim q_\psi(u|x, y, a)} \left[ \log(p_\psi(a|u)) \right]$$

where $\lambda_x$, $\lambda_y$, $\lambda_{MMD}$, $\lambda_{ADV}$ are scalar hyperparameters. Compared to existing approaches presented in previous section, the difference is the last term which corresponds to the expectation of the log-likelihood of $A$ given $U$ according to the decoder with parameters $\phi$. This decoder corresponds to a neural network which outputs the parameters of the distribution of $A$ given $U$ (i.e., the logits of a Categorical distribution for the discrete case, the mean and variances of a diagonal Gaussian in the continuous case).

All parameters are learned conjointly. Figure 2 gives the full architecture of our variational adversarial inference for the causal model from figure 1. It depicts the neural network encoder $q_\psi(U|X, Y, A)$ which generates a latent code $U$ from the inputs $X$, $Y$ and $A$. A neural network decoder $p_\theta(X, Y|U)$ reconstructs the original $X$ and $Y$ from both $U$ and $A$. The adversarial network $p_\psi$ tries to reconstruct the sensitive attribute $A$ from the confounder $U$. As classically done in adversarial learning, we alternate steps for the adversarial maximization and steps of global loss minimization (one gradient descent iteration on the same batch of data at each step). Optimization is done via the re-parametrization trick [50] to handle stochastic optimization.

2) Step 2: Counterfactual predictive model: As described in section 2.3, the counterfactual fairness in the predictive model learned at step 2 is ensured by comparing, for each training individual, counterfactual predictions $Y_{A \leftarrow a'}$ for all $a' \in \Omega_A$. For the discrete case (i.e., $A$ is a Categorical variable), we keep this process for our experiments. However, for the continuous setting (i.e., $A$ is for instance generated from a Gaussian), such an approach must be somehow adapted, due to the infinite set $\Omega_A$. In that case, we can consider a sampling distribution $P'(A)$ to formulate the following loss, which can be optimized via Monte-Carlo sampling and stochastic gradient descent (SGD):

$$L_{CF}(\theta) = \frac{1}{m} \sum_{i} \mu_i (h_\theta(x_i), y_i)$$

$$+ \lambda \mathbb{E}_{u \sim P(u|x, a, y_i), \tilde{x} \sim P(x|u, a_i), \tilde{a}' \sim P(a)|u, a', x'} \left[ (h_\theta(x) - h_\theta(x'))^2 \right]$$

This formulation is equivalent to the one from Eq. 3 for continuous outcomes $Y$ (thus considering a least squared cost as $\Delta$) and for continuous attributes $A$ (thus using the sampling distribution $P'(A)$ rather than considering every possible $a \in \Omega_A$).

Note that using a non-uniform sampling distribution $P'(A)$ would enforce the attention of the penalisation near the mass of the distribution. This prevents using the prior of $A$ estimated from the training set, since this would tend to reproduce inequity between individuals: counterfactual predictions for rare $A$ values would be little taken into account during training.

We therefore consider a uniform $P'(A)$ in our experiments for the continuous setting when using the $L_{CF}(\theta)$ objective at step 2.

However, for the specific case of high-dimensional sensitive attributes $A$, using a uniform sampling distribution $P'(A)$ could reveal as particularly inefficient. The risk is that a high number of counterfactual samples fall in easy areas for the learning process, while some difficult areas - where an important work for fairness has to be performed - remain insufficiently visited.

To tackle this problem, we propose to allow the learning process to dynamically focus on the most useful areas of $\Omega_A$ for each individual. During learning, we consider an adversarial process, which is in charge of moving the sampling distribution $P'(A)$, so that the counterfactual loss is the highest. This allows the learning process to select useful counterfactuals for ensuring fairness. Who can do more can do less: dynamically focusing on hardest areas allows one to avoid the enumeration of possible values in $\Omega_A$.

As described in section 2.3, the counterfactual fairness in the predictive model learned at step 2 is ensured by comparing, for each training individual, counterfactual predictions $Y_{A \leftarrow a'}$ for all $a' \in \Omega_A$. For the discrete case (i.e., $A$ is a Categorical variable), we keep this process for our experiments. However, for the continuous setting (i.e., $A$ is for instance generated from a Gaussian), such an approach must be somehow adapted, due to the infinite set $\Omega_A$. In that case, we can consider a sampling distribution $P'(A)$ to formulate the following loss, which can be optimized via Monte-Carlo sampling and stochastic gradient descent (SGD):

$$L_{CF}(\theta) = \frac{1}{m} \sum_{i} \mu_i (h_\theta(x_i), y_i)$$

$$+ \lambda \mathbb{E}_{u \sim P(u|x, a, y_i), \tilde{x} \sim P(x|u, a_i), \tilde{a}' \sim P(a)|u, a', x'} \left[ (h_\theta(x) - h_\theta(x'))^2 \right]$$

This formulation is equivalent to the one from Eq. 3 for continuous outcomes $Y$ (thus considering a least squared cost as $\Delta$) and for continuous attributes $A$ (thus using the sampling distribution $P'(A)$ rather than considering every possible $a \in \Omega_A$).

Note that using a non-uniform sampling distribution $P'(A)$ would enforce the attention of the penalisation near the mass of the distribution. This prevents using the prior of $A$ estimated from the training set, since this would tend to reproduce inequity between individuals: counterfactual predictions for rare $A$ values would be little taken into account during training.

We therefore consider a uniform $P'(A)$ in our experiments for the continuous setting when using the $L_{CF}(\theta)$ objective at step 2.

However, for the specific case of high-dimensional sensitive attributes $A$, using a uniform sampling distribution $P'(A)$ could reveal as particularly inefficient. The risk is that a high number of counterfactual samples fall in easy areas for the learning process, while some difficult areas - where an important work for fairness has to be performed - remain insufficiently visited.

To tackle this problem, we propose to allow the learning process to dynamically focus on the most useful areas of $\Omega_A$ for each individual. During learning, we consider an adversarial process, which is in charge of moving the sampling distribution $P'(A)$, so that the counterfactual loss is the highest. This allows the learning process to select useful counterfactuals for ensuring fairness. Who can do more can do less: dynamically focusing on hardest areas allows one to expect fairness everywhere. Again, we face a two-players adversarial game, which formulates as follows:

$$\arg\min_{\theta} \arg\max_{\phi} L_{DynCF}(\theta, \phi)$$

with:

$$L_{DynCF}(\theta, \phi) = \frac{1}{m} \sum_{i} \mu_i (h_\theta(x_i), y_i)$$

$$+ \lambda \mathbb{E}_{u \sim P(u|x, a, y_i), \tilde{x} \sim P(x|u, a_i), \tilde{a}' \sim P(a)|u, a', x'} \left[ (h_\theta(x) - h_\theta(x'))^2 \right]$$

Compared to Eq. 3 this formulation considers an adversarial sampling distribution $P'_\phi(A|U)$ rather than a uniform static distribution $P'(A)$. It takes the form of a neural network that outputs the parameters of the sampling distribution for a given
individual representation $U$. In our experiments we use a diagonal logit-Normal distribution $\text{sigmoid}(\mathcal{N}(\mu_x(u), \sigma^2_x(u)))$, where $\mu_x(u)$ and $\sigma^2_x(u)$ stand for the mean and variance parameters provided by the network for the latent code $u$. Samples from this distribution are then projected on the support $\Omega_A$ via a linear mapping depending on the shape of the set. Passing $U$ as input for the network allows the process to define different distributions for different codes: according to the individual profiles, the unfair areas are not always the same. This also limits the risk that the adversarial process gets stuck in sub-optimums of the sensitive manifold. As done for adversarial learning in step 1, all parameters are learned conjointly, by alternating steps for the adversarial maximization and steps of global loss minimization. The re-parametrization trick is also used, for the adversarial optimization of $P_o(A|X)$.

### IV. Experiments

We empirically evaluate the performance of our contribution on 6 real-world data sets. For the discrete scenario and specifically in the binary case ($Y \in \{0, 1\}, A \in \{0, 1\}$), we use 3 different popular data sets: the Adult UCI income data set with a gender sensitive attribute (male or female), the COMPAS data set with the race sensitive attribute (Caucasian or not-Caucasian) and the Bank dataset with the age as sensitive attribute (age is between 30 and 60 years, or not). For the continuous setting ($Y$ and $A$ are continuous), we use the 3 following data sets: the US Census dataset with gender rate as sensitive attribute encoded as the percentage of women in the census tract, the Motor dataset with the driver’s age as sensitive attribute and the Crime dataset with the ratio of an ethnic group per population as sensitive attribute.

Additionally to the 6 real-world datasets, we consider a synthetic scenario, that allows us to perform a further analysis of the relative performances of the approaches. The synthetic scenario subject is a pricing algorithm for a fictional car insurance policy, which follows the causal graph from figure 1. We simulate both a binary and a continuous dataset from this scenario. For both of them, 5000 individuals are sampled.

Details of distributions used for the continuous setting of this synthetic scenario are given below:

$$
Y \sim \mathcal{N}(7 + 0.1 * A + U_1 + U_2 + U_3, 1);
X_2 \sim \mathcal{N}(80 + A + U_2^2, 10);
X_3 \sim \mathcal{N}(200 + 5 * A + 5 * U_3, 20);
X_4 \sim \mathcal{N}((10^4 + 5 * A + U_4 + U_5, 1000)
X \sim [X_1, X_2, X_3, X_4];
A \sim \mathcal{N}[45, 5];
Y \sim \mathcal{N}(2 * (7 * A + 20 * \sum U_j), 0.1)
$$

### A. Step 1: Counterfactual Inference

In this section, we report experiments performed for assessing our adversarial approach for Counterfactual Inference (step 1 of the previous section). We compare our adversarial approach with two version of the approach in Eq. 3 each using one of the two MMD constraints MMD wrt $P(A)$ or MMD wrt $U_a$ as presented in section II-B (step 1). Note that these approaches are not applicable for continuous datasets as discussed at the end of section II. For every approach, we compare three different inference schemes for $U$: $q_x(u|x, y, a)$, $q_x(u|x, y)$ and $q_x(u|x, a)$. As a baseline, we also use a classical Variational Autoencoder inference without counterfactual independence constraint (i.e., Eq. II-B) without the last term).

All hyper-parameters for every approach have been tuned by 5-fold cross-validation. For the US Census data set for our approach for instance, the encoder $q_x$ architecture is an MLP of 3 hidden layers with 128, 64 and 32 units respectively, with ReLU activations. On this dataset, the decoder $p_y$ is an MLP of only one hidden layer with 64 units with a ReLu activation function and the output consists in one single output node with linear activation to reconstruct $Y$ and 37 units to reconstruct $X$ (number of features). The adversarial neural network $p_x$ is an MLP of two hidden layers with 32 and 16 units respectively. For the binary datasets, a sigmoid is applied on the outputs of decoders for $A$ and $Y$. For both MMD constraints we used a Gaussian radial basis function kernel. For all datasets, the prior distribution $p(U)$ considered for training the models is a five-dimensional standard Gaussian.

In order to evaluate the level of dependence between the latent space $U$ and the sensitive variable $A$, we compare the different approaches by using the neural estimation of the $HGR$ correlation coefficient given in [12]. This coefficient, as shown above in Eq 1, assesses the level of non-linear dependence between $X$ and $A$. This allows us to measure the dependency, both before (step 1) and after (step 2) the adversarial process. The $HGR$ correlation coefficient is defined as:

$$
HGR = \frac{\text{cov}(X, A)}{\sqrt{\text{var}(X) \text{var}(A)}}
$$

where $\text{cov}(X, A)$ is the covariance between $X$ and $A$, $\text{var}(X)$ is the variance of $X$ and $\text{var}(A)$ is the variance of $A$. The $HGR$ correlation coefficient is a measure of the linear dependence between $X$ and $A$. A value of $HGR$ close to 1 indicates a strong linear dependence, while a value close to 0 indicates a weak or non-existent linear dependence.
dependency between two jointly distributed random variables. The estimator is trained for each dataset and each approach on the train set, comparing observed variables $A$ with the corresponding inferred codes $U$.

For all data sets, we repeat five experiments by randomly sampling two subsets, 80% for the training set and 20% for the test set. Finally, we report the average reconstruction loss for $X$ and $Y$ on the test set, as long as the HGR between inferred test codes and the corresponding sensitive attributes. Results of our experiments can be found in Table I for the discrete case and Table II for the continuous case. For all of them, we attempted via the different hyperparameters ($\lambda_\phi$, $\lambda_y$, $\lambda_{MMD}$, $\lambda_{ADV}$) to obtain the lower dependence measure while keeping the minimum loss as possible to reconstruct $X$ and $Y$.

As expected, the baseline without the independence constraint achieves the best $X$ and $Y$ reconstruction loss, but this is also the most biased one with the worst dependence in terms of HGR in most datasets. Comparing the different constraints in the discrete case, the adversarial achieves globally the best result with the lower HGR while maintaining a reasonable reconstruction for $X$ and $Y$. It is unclear which MMD constraint performs better than the other. We observe that the best results in terms of independence are obtained without the sensitive variable given as input of the inference network (inference only with $X$ and $Y$). Note however that for the MMD constraints, this setting implies to make the wrong assumption of independence of $U$ w.r.t. $A$ given $X$ and $Y$ for the estimation of the constraint (as discussed at the end of Section II). This is not the case for our adversarial approach, which obtains particularly good results on this setting for discrete datasets. On continuous datasets, our approach succeeds in maintaining reasonable reconstruction losses for important gains in term of HGR compared to the classical VAE approach (without constraint). Interestingly, on these datasets, it appears that our approach obtains slightly better results when using the full information ($X$, $Y$ and $A$) as input of the inference network. We explain this by the fact that removing the influence of a binary input is harder than the one of a smoother continuous one, while this can reveal as a useful information for generating relevant codes.

### B. Step 2: Counterfactual predictive model

This section reports experiments involving the training procedure from step 2 as described in Section II-B. The goal of these experiments is threefold: 1. assess the impact of the adversarial inference on the target task of counterfactual fairness, 2. compare our two proposals for counterfactual bias mitigation (i.e., using a uniform distribution or an adversarial dynamic one for the sampling of counterfactual sensitive values) and 3. assess the impact of the control parameter from Eq. [9].

The predictive model used in our experiments is a MLP with 3 hidden layers. The adversarial network $P_\phi$ from Eq. [10] is a MLP with 2 hidden layers and RELU activation. For all our experiments, a single counterfactual for each individual is sampled at each iteration during the training of the models. Optimization is performed using ADAM.

Tables III and IV report results for the discrete and the continuous case respectively. The inference column refers to the inference process that was used for sampling counterfactuals for learning the predictive model. For each setting, we use the best configuration from Table II. The mitigation column refers to the type of counterfactual mitigation that is used for the results: No mitigation or $L_{CF}$ (Eq. [5]) for the discrete case; No mitigation, $L_{CF}$ (Eq. [5]) or $L_{DynCF}$ (Eq. [10]) for the continuous setting. Results are reported in terms of accuracy (for the discrete case) or MSE (for the continuous case) and of Counterfactual Fairness (CF). The CF measure is defined, for the $m_{test}$ individuals from the test set, as:

$$CF = \frac{1}{m_{test}} \sum_{i=1}^{m_{test}} \mathbb{E}_{(x', a') \sim C(i)}[\Delta(h_\theta(x_i, a_i), h_\theta(x', a'))]$$

where $C(i)$ is the set of counterfactual samples for the $i$-th individual of the test set. This corresponds to counterfactuals sampled with the Adversarial inference process defined at step 1 (with the best configuration reported in Tables II and III). As discussed above, the synthetic datasets allow one to rely on “true” counterfactuals for the computation of counterfactual fairness, rather than relying on an inference process which may include some bias. For these datasets, we thus also report an additional RealCF metric, which is defined as in Eq. [11] but using these counterfactuals sampled from the true codes used to generate the test data. For both CF and RealCF, for every $i$ from the test set, $|C(i)|$ equals 1 for binary settings and $|C(i)|$ equals 1000 for the continuous one. $\Delta$ is a cost function between two predictions, the logit paring cost for the binary case (more details given in section II-B step 2) and a simple squared difference for the continuous setting.

Results from both tables first confirm the good behavior of our inference model from step 1, which allows one to obtain greatly better results than other inference processes for both the discrete and the continuous settings. Our adversarial counterfactual inference framework allows one to get codes that can be easily used to generate relevant counterfactual individuals. For this observation, the most important results are those given for the synthetic scenarios, for which the RealCF metric shows good results for our method, while strongly reliable since relying on counterfactuals sampled from true codes of individuals.

Secondly, results from Table II show that, even in the continuous setting where the enumeration of all values from $\Omega_A$ is not possible, it is possible to define counterfactual mitigation methods such as our approaches $L_{CF}$ and $L_{DynCF}$. These two methods, used in conjunction with our Adversarial Inference, give significantly better results than no mitigation on every dataset. Interestingly, we also observe that $L_{DynCF}$ allows one to improve results over $L_{CF}$, which shows the relevance of the proposed dynamic sampling process. Furthermore, note that we can reasonably expect even better results compared to $L_{CF}$ on data with higher-dimensional sensitive attributes.

To illustrate the impact of the hyperparameter $\lambda$ on the predictions accuracy (MSE Error) and the counterfactual fairness
(a) $\lambda = 0.00$ ; $CF = 72\%$
(b) $\lambda = 0.10$ ; $CF = 44\%$
(c) $\lambda = 0.30$ ; $CF = 04\%$

Figure 3: Impact of $\lambda$ (Crime data set) on a specific instance $i$. Blue points are counterfactual predictions $h_\theta(x_{i,A\rightarrow a'})$ from 1.000 points $A \leftarrow a'$ generated randomly. The red cross represents the prediction $h_\theta(x_{i,A\rightarrow a})$ for the real $A = a$ of instance $i$.

| Table I: Inference results in the discrete case |
|---------------------------------------------|
| ![Image of Table I](image-url) |

estimation (CF), we plot results for 10 different values of $\lambda$ (5 runs each) on figure 4 for the Crime data set. It clearly confirms that higher values of $\lambda$ produce fairer predictions, while a value near 0 allows one to only focus on optimizing the predictor loss. This is also observable from Fig. 3 which plots counterfactual predictions for a specific instance $i$ from the test set. Higher values of $\lambda$ produce clearly more stable counterfactual predictions.

In figure 5 we consider the distribution of considered counterfactual samples w.r.t. to the sensitive variable $A$ for the uniform sampling strategy from $P(A)$ and the dynamic strategy as defined in Eq. 3. This is done on the Motor dataset and for a specific randomly sampled instance $i$ with sensitive attribute $a_1 = 75$, at a given point of the optimization, far before convergence (the model is clearly unfair at this point). The blue points are the counterfactual fairness estimation ($h_\theta(X_{i,A\rightarrow a}, a) - h_\theta(X_{i,A\rightarrow a'}, a')$) for each counterfactual sampled $a'$’s (1.000 points) from the uniform distribution $P(A)$. The red points are the counterfactual fairness estimations for counterfactuals corresponding to $a'$ values (30 points) sampled from our dynamic distribution $P_\phi(a'|u) = \mathcal{N}(\mu_\phi(u), \sigma_\phi^2(u))$, where $\phi$ are the parameters of the adver-
Table III: Counterfactual Fairness Results for the Discrete Case

| Inference           | Mitigation | Adult UCI | Compas | Bank   | Synthetic Scenario |
|---------------------|------------|-----------|--------|--------|--------------------|
|                     |            | Accuracy  | CF     | Accuracy | CF     | Accuracy  | CF    | Real CF   |
| Without Constraint  | None       | 84.22%    | 0.9096 | 67.12%  | 0.0102 | 90.64%   | 0.0369 | 99.49%    | 0.1087 | 0.1810   |
|                     | $L_{CF}$   | 83.28%    | 0.9008 | 66.20%  | 0.0051 | 90.46%   | 0.0024 | 95.89%    | 0.0757 | 0.1327   |
| $MMD$               | None       | 84.22%    | 0.0116 | 67.12%  | 0.0076 | 90.64%   | 0.0469 | 99.49%    | 0.1074 | 0.1775   |
|                     | $L_{CF}$   | 83.84%    | 0.0024 | 65.91%  | 0.0041 | 90.64%   | 0.0043 | 99.29%    | 0.0893 | 0.1557   |
| Adversarial         | None       | 84.22%    | 0.0114 | 67.12%  | 0.0118 | 90.64%   | 0.0376 | 99.49%    | 0.1426 | 0.1838   |
|                     | $L_{CF}$   | 83.74%    | 0.0002 | 66.73%  | 0.0004 | 90.60%   | 0.0000 | 93.19%    | 0.0001 | 0.0014   |

Table IV: Counterfactual Fairness Results for the Continuous Case

| Inference            | Mitigation | US Census | Motor   | Crime  | Synthetic Scenario |
|----------------------|------------|-----------|---------|--------|--------------------|
|                      |            | Accuracy  | CF      | MSE    | CF     | Accuracy  | CF    | MSE    | CF     | Real CF |
| Adversarial          | None       | 0.274     | 0.0302  | 0.938  | 0.0256 | 0.412     | 0.7412 | 0.484  | 0.0121 | 0.9546  |
|                      | $L_{CF}$   | 0.289     | 0.0005  | 0.941  | 0.0000 | 0.452     | 0.0154 | 0.572  | 0.0014 | 0.2013  |
|                      | $L_{DynCF}$| 0.290     | 0.0008  | 0.940  | 0.0005 | 0.445     | 0.0076 | 0.568  | 0.0013 | 0.2000  |
| Without Constraint   | None       | 0.274     | 0.0033  | 0.938  | 0.0271 | 0.381     | 0.7219 | 0.454  | 0.2919 | 1.1338  |
|                      | $L_{CF}$   | 0.307     | 0.0010  | 0.939  | 0.0021 | 0.407     | 0.2938 | 0.531  | 0.1968 | 0.3303  |
|                      | $L_{DynCF}$| 0.310     | 0.0008  | 0.942  | 0.0016 | 0.418     | 0.2881 | 0.546  | 0.1743 | 0.3188  |

Figure 5: Dynamic Sampling Visualization for a randomly sampled individual whose age $A$ is 75. Red points are sampled counterfactuals from the dynamic distribution $P_\phi(a'|u)$ with $u$ the inferred confounding for this individual.

V. CONCLUSION

We developed a new adversarial learning approach for counterfactual fairness. To the best of our knowledge, this is the first such method that can be applied for continuous sensitive attributes. The method proved to be very efficient for different dependence metrics on various artificial and real-world data sets, for both the discrete and the continuous settings. Finally, our proposal is applicable for any causal graph to achieve generic counterfactual fairness. As future works, it might be interesting to consider a generalization of our proposal for Path Specific [7] counterfactual fairness in the continuous case.

REFERENCES

[1] 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, pp. 4349–4357.
[2] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, “Machine bias. ProPublica, May 23, 2016,” 2016.
[3] D. Pedreshi, S. Ruggieri, and F. Turini, “Discrimination-aware data mining,” in KDD’08, 2008, pp. 560–568.
[4] T. Calder, F. Kamiran, and M. Pechenizkiy, “Building classifiers with independency constraints,” in ICDM Workshops. IEEE, 2009, pp. 13–18.
[5] M. B. Zafar, I. Valera, M. G. Rodriguez, and K. P. Gummadi, “Fairness constraints: Mechanisms for fair classification,” arXiv preprint arXiv:1507.05259, 2015.
[6] M. J. Kusner, J. Loftus, C. Russell, and R. Silva, “Counterfactual fairness,” in Advances in Neural Information Processing Systems, 2017, pp. 4066–4076.
[7] S. Chiappa, “Path-specific counterfactual fairness,” in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, 2019, pp. 7801–7808.
[8] J. H. Hinnefeld, P. Cooman, N. Mammo, and R. Deese, “Evaluating fairness metrics in the presence of dataset bias,” arXiv preprint arXiv:1809.09245, 2018.
[9] M. Hardt, E. Price, and N. Srebro, “Equality of opportunity in supervised learning,” in Advances in neural information processing systems, 2016, pp. 3315–3323.
[10] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, “Fairness through awareness,” in ITCS’12, 2012, pp. 214–226.
[45] I.-C. Yeh and C.-h. Lien, “The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients,” Expert Syst. Appl., vol. 36, no. 2, pp. 2473–2480, Mar. 2009.