Are demographically invariant models and representations in medical imaging fair?

Petersen, Eike; Ferrante, Enzo; Ganz, Melanie; Feragen, Aasa

Publication date:
2023

Citation for published version (APA):
Are demographically invariant models and representations in medical imaging fair?

Eike Petersen,1, 2, * Enzo Ferrante,3 Melanie Ganz,2, 4, 5 and Aasa Feragen1, 2

1 Technical University of Denmark, DTU Compute
2 Pioneer Centre for AI, Denmark
3 Research Institute for Signals, Systems and Computational Intelligence (CONICET), Universidad Nacional del Litoral, Argentina
4 University of Copenhagen, Department of Computer Science, Denmark
5 Neurobiology Research Unit, Rigshospitalet, Copenhagen, Denmark

*Corresponding author. Contact: ewipe@dtu.dk.

Abstract

Medical imaging models have been shown to encode information about patient demographics (age, race, sex) in their latent representation, raising concerns about their potential for discrimination. Here, we ask whether it is feasible and desirable to train models that do not encode demographic attributes. We consider different types of invariance with respect to demographic attributes – marginal, class-conditional, and counterfactual model invariance – and lay out their equivalence to standard notions of algorithmic fairness. Drawing on existing theory, we find that marginal and class-conditional invariance can be considered overly restrictive approaches for achieving certain fairness notions, resulting in significant predictive performance losses. Concerning counterfactual model invariance, we note that defining medical image counterfactuals with respect to demographic attributes is fraught with complexities. Finally, we posit that demographic encoding may even be considered advantageous if it enables learning a task-specific encoding of demographic features that does not rely on human-constructed categories such as ‘race’ and ‘gender’. We conclude that medical imaging models may need to encode demographic attributes, lending further urgency to calls for comprehensive model fairness assessments in terms of predictive performance.

1 Introduction

Recent studies have highlighted the capability of deep neural networks to infer patient demographics from medical images [8, 10, 11, 33]. In a widely cited study, Gichoya et al. [10] found that neural networks can be trained to recognize a patient’s race from chest X-ray recordings with high accuracy, even when medical doctors cannot, and even when correcting for confounding factors that correlate with racial identity. Prompted by this work, Glocke et al. [11] observed that even networks trained for chest X-ray-based disease classification (and not for inferring patient demographics) tend to learn a latent image encoding that differs in distribution between demographic groups. Both studies warn that the ability and apparent tendency of such networks to encode patient identity enables – intentional or unintentional – explicit discrimination against demographic groups: if the latent representation encodes group membership, the model can exploit this in its decision-making. For example, the model might learn to exploit spurious correlations between demographic groups and outcomes in the training dataset, which do not hold on another (real-world) dataset. These cautionary notes are timely and consequential, and they prompt the question: can and should we develop models that do not encode group membership in their latent space?
Here, we add to this ongoing discussion by considering different types of demographic invariance and assessing their relationship to notions of algorithmic fairness, as well as their desirability in the medical imaging domain. First, we consider marginal representation invariance, corresponding to a latent space that does not encode group membership (section 2). We point out that marginal invariance implies statistical parity, discussing why this is undesirable in virtually all medical imaging applications. Secondly, we consider class-conditional representation invariance, which implies the separation fairness criterion (section 3). We lay out why enforcing this criterion appears undesirable as well (section 4). Figure 1 shows an illustration of the two representation invariance approaches. Finally, we consider counterfactual model invariance, corresponding to counterfactual fairness (section 5). We discuss the challenges involved in defining meaningful counterfactuals with respect to demographic groups in medical imaging, finding that this notion appears impractical. Our negative findings lend further urgency to the development and implementation of thorough fairness assessments, given that models will have the capability to discriminate against demographic groups.

The technical results we discuss are not new; references are provided throughout. Our aim is to emphasize the relevance of these results to the current discourse in (fair) medical imaging, and explore their practical implications.

1.1 Problem setting and notation

We consider a supervised prediction setting in which the objective is to predict labels $Y$ from inputs $X$. Patients are assumed to be members of different and potentially overlapping demographic groups $A$ (e.g., young, female, and young female). The inputs $X$ might denote medical images, blood markers, or other physiological measurements, and the labels $Y$ could, e.g., represent categorical disease labels, continuous disease severity scores, or segmentation masks. We often consider a latent representation $Z$ obtained using a deterministic feature extractor $g : x \mapsto z$, such as the first layers of a deep neural network. This latent representation is then mapped onto predictions $r \in \mathbb{R}^{\dim(Y)}$ by a second deterministic model component $h : z \mapsto r$. Depending on the application, $r$ may then be discretized using a decision threshold $\tau$ to obtain binary outcome labels $\hat{y}$ representing, for example, disease labels or segmentation masks. Neither $g$ nor $h$ receive group membership as an explicit input, and we assume $r$ to be group-independent. We will refer to random variables by upper-case letters ($X, Y, Z$) and to their
realizations by lower-case letters (x, y, z). We consider a model to “encode” group membership $A$ in its latent representation $Z$ if group membership can be inferred with higher-than-chance accuracy from $Z$.

## 2 Marginal representation invariance

Aiming for a model that does not encode group membership is equivalent to requiring the latent representation $z$ to be invariant between groups $a$, that is,

$$p(z) = p(z \mid a) \quad \forall a \iff Z \perp A.$$  \hspace{1cm} (1)

However, if $p(z \mid a)$ is identical across groups, then the distributions of model predictions $p(r \mid a)$ and $p(\hat{y} \mid a)$ are identical across groups as well, implying $R, Y \perp A$. This corresponds to the algorithmic fairness notion of statistical parity, or independence $\[3, 35\]$. If, however, the true outcome distributions $p(y \mid a)$ differ between groups, we cannot require $p(\hat{y} \mid a \neq p(y \mid a)$ necessarily $\[9, 12, 27\]$.

Why would $p(y \mid a)$ differ between groups in a medical application? In the simplest case, prevalence could differ. A classifier that returns the same distribution of positive and negative predictions for breast cancer in men and women appears undesirable as the prevalence of breast cancer differs between these groups. If, on the other hand, the classifier returns positive and negative predictions at different rates for the different groups (as would be correct), then its latent representation is statistically related to group membership, thus “encoding” group membership. As another example from medical image segmentation, organ shapes or sizes may vary depending on age or sex, resulting in differences in the distribution $p(y \mid a)$ of true segmentation masks between groups $\[24\]$.

In domain adaptation theory, property (1) is called marginal alignment, and a latent representation that satisfies it is often called domain-invariant. Extensive research has been devoted to domain-invariant representation learning, and by identifying different groups with different domains, these results apply to our setting. The equality of $p(y \mid a)$ between groups is known to be a necessary condition for the existence of a predictive performance-optimal (marginally) invariant representation $\[18, 35\]$. Similarly, the field of algorithmic fairness has widely discussed the inherent tensions between statistical parity and predictive accuracy. Enforcing statistical parity despite differences in $p(y \mid a)$ is known to incur a significant loss in predictive performance $\[3, 9, 21, 35\]$. For binary classification with two sensitive groups, Zhao et al. $\[35\]$ show that enforcing statistical parity implies that the sum of the error rates in both groups is lower-bounded by the prevalence difference.

To provide some intuition concerning the theoretical results presented in this section, note that there is a crucial difference between a model (i.e., a function) and a representation being invariant with respect to a demographic feature. The former asserts that the prediction $\hat{y}$ should be the same regardless of the value of $A$ while keeping everything else fixed; we will explore this notion in more detail in section 5. Importantly, this still allows for the predictions $\hat{Y}$ and group membership $A$ to be correlated if A correlates with disease-relevant features. An invariant representation, on the other hand, requires full statistical independence $Z, \hat{Y} \perp A$, even if the labels $Y$ are (spuriously) correlated with $A$. In this case, a demographically invariant representation requires actively confounding predictions to comply with the invariance requirement, forcing unnecessary misclassification in all groups. (In the case of differing $p(y \mid a)$, a perfect classifier that predicts all labels correctly does not satisfy marginal independence.)

In the case of low-dimensional labels such as disease labels, there is one obvious strategy for addressing the challenges posed by label shift for marginal invariance approaches: One can artificially balance the training set such that $p(y \mid a)$ is equal across groups. In some cases, one may also consider prevalence differences between groups negligible or purely an artifact of biased data collection procedures. Would enforcing a demographically invariant representation appear beneficial in such cases? We will return to this question in section 4, where we discuss more general drawbacks of representation invariance approaches.
3 Class-conditional representation invariance

The situation in which \( p(y \mid a) \) differs between domains is known as label shift [7, 17], and various methods have been developed to address it. One class of proposed solutions [7, 18] attempts to match the class-conditional distributions \( p(z \mid y) \) across groups, instead of the marginal distributions \( p(z) \) like in the previous section. Formally, this requirement can be stated as

\[
p(z \mid y) = p(z \mid y, a) \quad \forall a, y \iff Z \perp A \mid Y.
\]

Analogously to the previous section, observe that eq. (2) implies equality of \( p(r \mid y, a) \) and \( p(\hat{y} \mid y, a) \) across groups, and thus \( R, \hat{Y} \perp A \mid Y \). This corresponds to the separation criterion in algorithmic fairness [3]. Note that class-conditional representation invariance does not imply marginal representation invariance, i.e., models that satisfy eq. (2) may encode group membership in their latent space.

Is class-conditional representation invariance a desirable property for medical imaging models? We argue here that this is not the case, even leaving aside the fact that group membership may be encoded. It is known that a risk score \( R \) cannot satisfy separation and be well-calibrated by groups at the same time, except in pathological cases [3]. For this reason, and because its intrinsic ethical significance appears unclear, it has been argued that separation at the risk score level (\( R \perp A \mid Y \)) may not be a desirable model property [13, 16, 25]. Notably, this is distinct from separation at the classification level (\( \hat{Y} \perp A \mid Y \)), which entails equal error rates between groups and may be a desirable aim. However, as has been pointed out elsewhere [16, 25], error rate equality can be achieved without the overly restrictive requirement of class-conditionally invariant risk distributions. Further fundamental drawbacks of both marginal and class-conditional representation invariance approaches are discussed in the following section.

4 General drawbacks of representation invariance

A key drawback of any notion of representation invariance concerns their neglect of differences in the within-class distributions between groups [17, 19]. A single class label often subsumes many fundamentally distinct situations, such as different subtypes or presentations of the disease, a phenomenon known as hidden stratification [23]. If the distribution of these subclass situations differs between groups, then representation invariance can only be achieved by forcing distinct stratifications in different groups to be represented by the same latent encoding. This is analogous to the higher-level effects of enforcing marginal invariance in the case of label shift, discussed in section 2. One instance of the within-class variation problem concerns differences in task difficulty. For physiological or technical reasons, a prediction task may be harder in one group than in others, due to, for example, differences in the amount of (breast, fat) tissue that confounds a recording [1, 5]. In this case, a predictive model should return less confident predictions for members of the more strongly confounded group, even for the same disease instance. Representation invariance approaches require the equalization of these essential differences between groups.

Do representation invariance approaches at least provide meaningful fairness guarantees? As we have seen, marginal invariance implies statistical parity, which may be a desirable goal in scarce resource distribution settings or patient prioritization [3, 25] but is typically not considered desirable in predictive settings. In this regard, Glocker et al. [11] also point out that if a representation encodes group membership, this does not imply that the model also uses this information for decision-making. Conditional invariance, on the other hand, implies equalized error rates, which may be a desirable aim in the predictive setting, even though its algorithmic enforcement is known to suffer from the leveling down phenomenon [34, 37]. Equalized error rates can also be achieved without requiring equalized conditional risk distributions, however [16, 25]. Thus, the conditional invariance requirement may be seen as overly restrictive, resulting in the noted incompatibility with calibration by groups.

At this point, let us ask: why were we interested in demographically invariant representations in the first place? Echoing similar concerns raised by Gichoya et al. [10], Glocker et al. [11] write that "an
algorithm may encode protected characteristics, and then use this information for making predictions due to undesirable correlations in the (historical) training data." These remarks reflect a concern that patients with similar (patho)physiology might wrongly receive different predictions if the model takes their demographic attributes into account. We argue that this concern is more aligned with requiring demographically invariant models, as opposed to demographically invariant distributions. We will thus consider model invariance approaches in the next section.

5 Model invariance

To address the drawbacks of invariant representation learning, there has been a shift in the field away from learning invariant representations toward learning invariant mechanisms, that is, models or model components that are, in some sense, invariant with respect to a nuisance variable $A$. One popular approach is based on the notion of counterfactual invariance: keeping everything else fixed, changing just the attribute $A$ should not change model predictions. When $A$ represents a sensitive attribute, this corresponds to notions of counterfactual fairness, a variant of individual fairness.

In theory, counterfactual invariance holds across datasets: if a model is invariant with respect to $A$, then this will still hold if the data distribution changes. The case of invariance with respect to demographic groups in medical imaging is particularly complex, however, and challenging to define formally. First, note that interesting connections have been observed between model invariance and the representation invariance approaches discussed earlier. Veitch et al. show that under a specific assumption regarding the causal relationships between features $A$, inputs $X$ and labels $Y$, counterfactual model invariance with respect to $A$ implies $R, Y \perp A \mid Y$, i.e., separation – just like in the case of class-conditional representation invariance. Puli et al. derive similar equivalences. These results might be considered surprising, given all the drawbacks of representation invariance discussed above, and given that model invariance seems like a fundamentally distinct approach. How do these equivalences arise?

The crux of counterfactual invariance approaches lies in the definition of counterfactuals. For example, Veitch et al. assume that taking a counterfactual by changing $a$ to $a'$ should entail adjusting all other covariates that are influenced by the property $A$, leaving unchanged only those properties that are only affected by the disease label $Y$. In a chest X-ray context, this might imply adjusting torso shapes, tissue distributions, organ sizes, and differing disease presentations to conform with the distribution observed in the group $a'$. Adjusting all of these factors when creating, for example, a ‘male counterfactual’ of a female image, yields a fully male-typical example – thus the equivalence to class-conditional representation invariance. This raises the question: What, precisely, would we like to keep fixed, and what should be adjusted, when generating ‘biological sex counterfactuals’, ‘ethnicity counterfactuals’, or ‘age counterfactuals’? Which are the peculiar properties of group $a$ with respect to which a model should be invariant, and which are mere correlates that we would permit to influence model decisions? These are highly nontrivial questions, particularly in the context of demographic groups in medical imaging. The validity of a counterfactual model invariance approach fully depends on the answers, however.

6 Discussion & Conclusion

Our starting point in this piece were observations by different research groups that deep learning models tend to encode patients’ demographic features in their latent space. Prompted by these observations, we first asked whether it is feasible and desirable to train models that do not encode demographic group membership, in the sense that it cannot be inferred with higher-than-chance accuracy from the latent representation. Noting that this requirement is equivalent to both marginal representation invariance and statistical parity, we showed how such a requirement can severely hurt model performance even beyond the well-known ‘leveling down’ effect. We
then considered a popular relaxation of marginal representation invariance, **class-conditional invariance** [7]. This notion alleviates one of the problems associated with marginal invariance: severe model performance deterioration in the face of label shift, i.e., differences in $p(y \mid a)$ between groups. However, class-conditional invariance turned out to imply the **separation criterion** from algorithmic fairness (on the risk score level), which is undesirable due to its incompatibility with group-wise calibration, as well as for other reasons [3, 13, 16, 25]. Moreover, all representation invariance approaches suffer from their neglect of differences in **intra-class variations** between groups due to, for example, different disease subtypes [17, 19, 23]. Finally, we considered counterfactually invariant **models** as one potential alternative [26, 31], finding that the definition of a meaningful demographic counterfactual in the medical imaging domain is fraught with serious challenges.

Can it even be **beneficial** for a model to encode group membership? Consider the case of a model that depends on explicit group membership information. The model might exploit such information during training – e.g., to achieve representation invariance – or during inference, in order to perform group-specific calibration or thresholding. Such a model inherits the well-documented problems that arise from sorting humans into categories based predominantly on **sociocultural** constructs [4, 30], as opposed to physiological differences relevant to the prediction task at hand. As an alternative, consider now the case of a model that has learned an **implicit** representation of group membership. This second model can learn to extract just those aspects of, say, ethnicity or biological sex that are relevant to the given prediction task. Moreover, it can learn a **continuous** representation of these properties, as opposed to coarse, human-defined categories. This might enable more robust generalization to patient groups that fall between traditional categories, such as nonbinary or mixed-race patients. To be clear: this is, of course, a highly idealized view. Whether a model indeed learns such a minimal and optimal representation in practice is an important question. Encouragingly, Glocker et al. [11] provide evidence that this may indeed happen in practice. They find that a model trained only for disease prediction, and not demographic group prediction, indeed appears to learn a feature representation that is far less predictive of demographic properties than the representation learned by a model trained explicitly for demographic group prediction.

While our discussion of representation invariance has been largely negative, we want to emphasize that such approaches are not without merit. Their main field of application is the unsupervised domain adaptation setting, in which labels are unavailable from a new domain. In this case, invariant representation learning can be beneficial [18, 22]. Notably, this differs from the setting we consider here, in which labels are available from all demographic groups. Nevertheless, such invariant representations might generalize better to previously unseen demographic groups, even though domain generalization benchmarks appear to refute this intuition [32]. Importantly, our discussion here concerned the case of enforcing **strict** invariance. In practice, many invariant representation learning approaches instead use **regularization** to prevent learning representations that are unnecessarily strongly predictive of the domain or demographic group [35]. Such approaches may prove beneficial if they are tuned to minimize the negative effects of enforcing strict invariance. In such a case, the latent representation will still encode demographic group membership to some degree, however.

Taken together, our analyses imply that, at present, there appears to be no straightforward method for developing medical imaging models that guarantee similar treatment of individuals with similar physiology but differing demographic features. Enforcing different notions of demographic invariance is likely to harm model performance across all groups, as has been observed empirically [34, 37]. As a consequence, we claim that the simple fact that a model encodes group membership cannot be understood as a fairness violation. Indeed, we have argued that group encoding can in some cases even be considered beneficial if it prevents models from inheriting the biases encoded in human-defined patient categories. Our analysis lends further urgency to calls for fairness assessments in terms of model predictions since, as pointed out before [10, 11], such models have the capacity to discriminate. For improving model performance in under-performing groups, simple balanced empirical risk minimization, targeted data collection efforts, and investigations into the potential presence of label biases currently appear to be among the most promising practical avenues [34].
Acknowledgements

Work on this project was partially funded by the Independent Research Fund Denmark (DFF, grant number 9131-00097B), Denmark’s Pioneer Centre for AI (DNRF grant number P1), a Google Award for inclusion research, the Novo Nordisk Foundation through the Center for Basic Machine Learning Research in Life Science (MILS, grant number NNF20OC0062606), and the Argentinian National Agency for the Promotion of Research, Technological Development and Innovation (ANPCyT, grant number PICT-PRH-2019-0000).

References


