

---

# COUNTERFACTUAL TRAINING: TEACHING MODELS PLAUSIBLE AND ACTIONABLE EXPLANATIONS

---

A PREPRINT

**Patrick Altmeyer** 

Faculty of Electrical Engineering, Mathematics and Computer Science  
Delft University of Technology

[p.altmeyer@tudelft.nl](mailto:p.altmeyer@tudelft.nl)

**Aleksander Buszydlik**

Faculty of Electrical Engineering, Mathematics and Computer Science  
Delft University of Technology

**Arie van Deursen**

Faculty of Electrical Engineering, Mathematics and Computer Science  
Delft University of Technology

**Cynthia C. S. Liem**

Faculty of Electrical Engineering, Mathematics and Computer Science  
Delft University of Technology

March 10, 2025

## ABSTRACT

We propose a novel training regime called Counterfactual Training that leverages counterfactual explanations to increase the explanatory capacity of models. Counterfactual explanations have emerged as a popular post-hoc explanation method for opaque machine learning models: they inform how factual inputs would need to change in order for a model to produce some desired output. To be useful in real-word decision-making systems, counterfactuals should be plausible with respect to the underlying data and actionable with respect to stakeholder requirements. Much existing research has therefore focused on developing post-hoc methods to generate counterfactuals that meet these desiderata. In this work, we instead hold models directly accountable for this desired end goal: Counterfactual Training employs counterfactuals ad-hoc during the training phase to minimize the divergence between learned representations and plausible, actionable explanations. We demonstrate empirically and theoretically that our proposed method facilitates training models that deliver inherently desirable explanations while maintaining high predictive performance.

**Keywords** Counterfactual Training • Counterfactual Explanations • Algorithmic Recourse • Explainable AI • Representation Learning

**1 Introduction**

Today's prominence of artificial intelligence (AI) has largely been driven by advances in **representation learning**: instead of relying on features and rules that are carefully hand-crafted by humans, modern machine learning (ML)

18 models are tasked with learning the representations directly from data, guided by narrow objectives such as predictive  
 19 accuracy (I. Goodfellow, Bengio, and Courville 2016). Modern advances in computing have made it possible to  
 20 provide such models with ever growing degrees of freedom to achieve that task, which has often led them to outperform  
 21 traditionally more parsimonious models. Unfortunately, in doing so, the models learn increasingly complex and highly  
 22 sensitive representations that we can no longer easily interpret.

23 The trend towards complexity for the sake of performance has come under serious scrutiny in recent years. At the  
 24 very cusp of the deep learning revolution, Szegedy et al. (2013) showed that artificial neural networks (ANN) are  
 25 sensitive to adversarial examples: counterfactuals of model inputs that yield vastly different model predictions despite  
 26 being “imperceptible” in that they are semantically indifferent from their factual counterparts. Although some partially  
 27 effective mitigation strategies have been proposed, for example **adversarial training** (I. J. Goodfellow, Shlens, and  
 28 Szegedy 2014), truly robust deep learning (DL) remains unattainable even for models that are considered shallow by  
 29 today’s standards (Kolter 2023).

30 Part of the problem is that the high degrees of freedom provide room for many solutions that are locally optimal with  
 31 respect to narrow objectives (Wilson 2020).<sup>1</sup> Indeed, recent work on the so called “lottery tickets” suggests that modern  
 32 neural networks can be pruned by up to 90% while preserving their predictive performance (Frankle and Carbin 2019)  
 33 and generalizability (Morcos et al. 2019). Similarly, Zhang et al. (2021) showed that state-of-the-art neural networks  
 34 are so expressive that they can fit randomly labeled data. Thus, looking at the predictive performance, the solutions may  
 35 seem to provide compelling explanations for the data, when in fact they are based on purely associative, semantically  
 36 meaningless patterns. This poses two related challenges. Firstly, there is no dependable way to verify if such complex  
 37 representations correspond to meaningful and plausible explanations. Secondly, even if we could resolve the first  
 38 challenge, it remains undecided how to ensure that models can *only* learn valuable explanations.

39 The first challenge has attracted an abundance of research on **explainable AI** (XAI) which aims to develop tools to  
 40 derive explanations from complex model representations. This can mitigate a scenario in which we deploy opaque  
 41 models and blindly rely on their predictions. On countless occasions, this scenario has occurred in practice and caused  
 42 real harm to people who were affected adversely and often unfairly by automated decision-making (ADM) systems  
 43 involving opaque models (O’Neil 2016; McGregor 2021). Effective XAI tools can aid us in monitoring models and  
 44 providing recourse to individuals to turn adverse outcomes (e.g., “loan application rejected”) into positive ones (e.g.,  
 45 “application accepted”). Wachter, Mittelstadt, and Russell (2017) propose **counterfactual explanations** (CE) as an  
 46 effective approach to achieve this goal: CEs explain how factual inputs need to change in order for some fitted model  
 47 to produce some desired output, typically involving minimal perturbations.

48 To our surprise, the second challenge has not yet attracted any major consolidated research effort. Specifically, there  
 49 has been no concerted effort towards improving models’ explanatory capacity, which we will henceforth  
 50 simply call “explainability”, defined as the degree to which learned representations correspond to explanations that are  
 51 interpretable and deemed **plausible** by humans (see Definition 3.1). Instead, the choice has typically been to improve  
 52 the ability of XAI tools to identify the subset explanations that are both plausible and valid for any given model,  
 53 independent of whether the learned representations are also compatible with implausible explanations (Altmeyer et  
 54 al. 2024). Fortunately, recent findings indicate that explainability can arise as byproduct of regularization techniques  
 55 aimed at other objectives such as robustness, generalization, and generative capacity (Schut et al. 2021; Augustin,  
 56 Meinke, and Hein 2020; Altmeyer et al. 2024).

57 Building on these findings, we introduce **counterfactual training**: a novel training regime explicitly geared towards  
 58 aligning model representations with plausible explanations. Our contributions are as follows:

- 59 • We discuss existing related work on improving models and consolidate it through the lens of counterfactual  
   explanations (Section 2).
- 60 • We present our proposed methodological framework that leverages faithful counterfactual explanations during  
   the training phase of models to achieve the explainability objective (Section 3).
- 61 • Through extensive experiments we demonstrate the counterfactual training improve model explainability  
   while maintaining high predictive performance. We run ablation studies and grid searches to understand  
   how the underlying model components and hyperparameters affect outcomes. (Section 4).

66 Despite some limitations of our approach discussed in Section 5, we conclude in Section 6 that counterfactual training  
 67 provides a practical framework for researchers and practitioners interested in making opaque models more trustworthy.  
 68 We also believe that this work serves as an opportunity for XAI researchers to re-evaluate the trend of improving XAI  
 69 tools without improving the underlying models.

---

<sup>1</sup>We follow the standard ML convention, where “degrees of freedom” refer to the number of parameters estimated from data.

## 70 2 Related Literature

71 To the best of our knowledge, our proposed framework of counterfactual training represents the first attempt to use  
 72 counterfactual explanations during training to improve model explainability. In high-level terms, we define model  
 73 explainability as the extent to which valid explanations derived for an opaque model are also deemed plausible with  
 74 respect to the underlying data and stakeholder requirements. To make this more concrete, we follow Augustin, Meinke,  
 75 and Hein (2020) in tying the concept of explainability to the quality of counterfactual explanations that we can generate  
 76 for a given model. The authors show that counterfactual explanations—understood here as minimal input perturbations  
 77 that yield some desired model prediction—are generally more meaningful if the underlying model is more robust to  
 78 adversarial examples. We can make intuitive sense of this finding when looking at adversarial training (AT) through  
 79 the lens of representation learning with high degrees of freedom: by inducing models to “unlearn” representations that  
 80 are susceptible to worst-case counterfactuals (i.e., adversarial examples), AT effectively removes some implausible  
 81 explanations from the solution space.

### 82 2.1 Adversarial Examples are Counterfactual Explanations

83 This interpretation of the link between explainability through counterfactuals on one side, and robustness to adversarial  
 84 examples on the other, is backed by empirical evidence. Sauer and Geiger (2021) demonstrate that using counterfactual  
 85 images during classifier training improves model robustness. Similarly, Abbasnejad et al. (2020) argue that counter-  
 86 factuals represent potentially useful training data in machine learning, especially in supervised settings where inputs  
 87 may be reasonably mapped to multiple outputs. They, too, demonstrate the augmenting the training data of image  
 88 classifiers can improve generalization. Teney, Abbasnejad, and Hengel (2020) propose an approach using counterfac-  
 89 tuals in training that does not rely on data augmentation: they argue that counterfactual pairs typically already exist  
 90 in training datasets. Specifically, their approach relies on identifying similar input samples with different annotations  
 91 and ensuring that the gradient of the classifier aligns with the vector between such pairs of counterfactual inputs using  
 92 the cosine distance as the loss function.

93 In the natural language processing (NLP) domain, counterfactuals have similarly been used to improve models through  
 94 data augmentation: Wu et al. (2021), propose *Polyjuice*, a general-purpose counterfactual generator for language mod-  
 95 els. They demonstrate empirically that augmenting training data through *Polyjuice* counterfactuals improves robust-  
 96 ness in a number of NLP tasks. Balashankar et al. (2023) also use *Polyjuice* to augment NLP datasets through diverse  
 97 counterfactuals and show that classifier robustness improves up to 20%. Finally, Luu and Inoue (2023) introduce  
 98 Counterfactual Adversarial Training (CAT), which also aims at improving generalization and robustness of language  
 99 models. Specifically, they propose to proceed as follows: firstly, they identify training samples that are subject to  
 100 high predictive uncertainty; secondly, they generate counterfactual explanations for those samples; and, finally, they  
 101 fine-tune the given language model on the augmented dataset that includes the generated counterfactuals.

102 There have also been several attempts at formalizing the relationship between counterfactual explanations and adver-  
 103 sarial examples (AE). Pointing to clear similarities in how CE and AE are generated, Freiesleben (2022) makes the  
 104 case for jointly studying the opaqueness and robustness problem in representation learning. Formally, AE can be seen  
 105 as the subset of CE for which misclassification is achieved (Freiesleben 2022). Similarly, Pawelczyk et al. (2022)  
 106 show that CE and AE are equivalent under certain conditions and derive theoretical upper bounds on the distances  
 107 between them.

108 Two recent works are closely related to ours in that they use counterfactuals during training with the explicit goal  
 109 of affecting certain properties of post-hoc counterfactual explanations. Firstly, Ross, Lakkaraju, and Bastani (2024)  
 110 propose a way to train models that are guaranteed to provide recourse for individuals to move from an adverse outcome  
 111 to some positive target class with high probability. Their approach builds on adversarial training, where in this context  
 112 susceptibility to targeted adversarial examples for the positive class is explicitly induced. The proposed method allows  
 113 for imposing a set of actionability constraints ex-ante: for example, users can specify that certain features (e.g., *age*,  
 114 *gender*, ...) are immutable. Secondly, Guo, Nguyen, and Yadav (2023) are the first to propose an end-to-end training  
 115 pipeline that includes counterfactual explanations as part of the training procedure. In particular, they propose a  
 116 specific network architecture that includes a predictor and CE generator network, where the parameters of the CE  
 117 generator network are learnable. Counterfactuals are generated during each training iteration and fed back to the  
 118 predictor network. In contrast to Guo, Nguyen, and Yadav (2023), we impose no restrictions on the neural network  
 119 architecture at all.

### 120 2.2 Beyond Robustness

121 Improving the adversarial robustness of models is not the only path towards aligning representations with plausible  
 122 explanations. In a work closely related to this one, Altmeyer et al. (2024) show that explainability can be improved  
 123 through model averaging and refined model objectives. The authors propose a way to generate counterfactuals that  
 124 are maximally **faithful** to the model in that they are consistent with what the model has learned about the underlying

125 data. Formally, they rely on tools from energy-based modelling to minimize the divergence between the distribution  
 126 of counterfactuals and the conditional posterior over inputs learned by the model. Their proposed counterfactual  
 127 explainer, *ECCo*, yields plausible explanations if and only if the underlying model has learned representations that  
 128 align with them. They find that both deep ensembles (Lakshminarayanan, Pritzel, and Blundell 2017) and joint energy-  
 129 based models (JEMs) (Grathwohl et al. 2020) tend to do well in this regard.

130 Once again it helps to look at these findings through the lens of representation learning with high degrees of freedom.  
 131 Deep ensembles are approximate Bayesian model averages, which are most called for when models are underspecified  
 132 by the available data (Wilson 2020). Averaging across solutions mitigates the aforementioned risk of relying on a  
 133 single locally optimal representations that corresponds to semantically meaningless explanations for the data. Previous  
 134 work by Schut et al. (2021) similarly found that generating plausible (“interpretable”) counterfactual explanations is  
 135 almost trivial for deep ensembles that have also undergone adversarial training. The case for JEMs is even clearer:  
 136 they involve a hybrid objective that induces both high predictive performance and generative capacity (Grathwohl et al.  
 137 2020). This is closely related to the idea of aligning models with plausible explanations and has inspired our proposed  
 138 counterfactual training objective, as we explain in Section 3.

### 139 3 Counterfactual Training

140 Counterfactual training combines ideas from adversarial training, energy-based modelling and counterfactuals expla-  
 141 nations with the explicit objective of aligning representations with plausible explanations that comply with user re-  
 142 quirements. In the context of CEs, plausibility has broadly been defined as the degree to which counterfactuals comply  
 143 with the underlying data generating process (Poyiadzi et al. 2020; Guidotti 2022; Altmeyer et al. 2024). Plausibility  
 144 is a necessary but insufficient condition for using CEs to provide algorithmic recourse (AR) to individuals affected  
 145 by opaque models in practice. This is because for recourse recommendations to be **actionable**, they need to not only  
 146 result in plausible counterfactuals but also be attainable. A plausible CE for a rejected 20-year-old loan applicant, for  
 147 example, might reveal that their application would have been accepted, if only they were 20 years older. Ignoring  
 148 all other features, this would comply with the definition of plausibility if 40-year-old individuals were in fact more  
 149 credit-worthy on average than young adults. But of course this CE does not qualify for providing actionable recourse  
 150 to the applicant since *age* is not a (directly) mutable feature. For our intents and purposes, counterfactual training aims  
 151 to improve model explainability by aligning models with counterfactuals that meet both desiderata, plausibility and  
 152 actionability. Formally, we define explainability as follows:

153 **Definition 3.1** (Model Explainability). Let  $M_\theta : \mathcal{X} \mapsto \mathcal{Y}$  denote a supervised classification model that maps from the  
 154  $D$ -dimensional input space  $\mathcal{X}$  to representations  $\phi(\mathbf{x}; \theta)$  and finally to the  $K$ -dimensional output space  $\mathcal{Y}$ . Assume  
 155 that for any given input-output pair  $\{\mathbf{x}, \mathbf{y}\}_i$  there exists a counterfactual  $\mathbf{x}' = \mathbf{x} + \Delta : M_\theta(\mathbf{x}') = \mathbf{y}^+ \neq \mathbf{y} = M_\theta(\mathbf{x})$   
 156 where  $\arg \max_y \mathbf{y}^+ = y^+$  and  $y^+$  denotes the index of the target class.

157 We say that  $M_\theta$  is **explainable** to the extent that faithfully generated counterfactuals are plausible (i.e. consistent with  
 158 the data) and actionable. Formally, we define these properties as follows:

- 159 1. (Plausibility)  $\int^A p(\mathbf{x}' | \mathbf{y}^+) d\mathbf{x} \rightarrow 1$  where  $A$  is some small region around  $\mathbf{x}'$ .
- 160 2. (Actionability) Permutations  $\Delta$  are subject to some actionability constraints.

161 We consider counterfactuals as faithful to the extent that they are consistent with what the model has learned about the  
 162 input data. Let  $p_\theta(\mathbf{x} | \mathbf{y}^+)$  denote the conditional posterior over inputs, then formally:

- 163 3. (Faithfulness)  $\int^A p_\theta(\mathbf{x}' | \mathbf{y}^+) d\mathbf{x} \rightarrow 1$  where  $A$  is defined as above.

164 The definitions of faithfulness and plausibility in Definition 3.1 are the same as in Altmeyer et al. (2024), with adapted  
 165 notation. Actionability constraints in Definition 3.1 vary and depend on the context in which  $M_\theta$  is deployed. In this  
 166 work, we focus on domain and mutability constraints for individual features  $x_d$  for  $d = 1, \dots, D$ . We limit ourselves  
 167 to classification tasks for reasons discussed in Section 5.

#### 168 3.1 Our Proposed Objective

169 Let  $\mathbf{x}'_t$  for  $t = 0, \dots, T$  denote a counterfactual explanation generated through gradient descent over  $T$  iterations  
 170 as initially proposed by Wachter, Mittelstadt, and Russell (2017). For our purposes, we let  $T$  vary and consider the  
 171 counterfactual search as converged as soon as the predicted probability for the target class has reached a pre-determined  
 172 threshold,  $\tau : \mathcal{S}(M_\theta(\mathbf{x}'))[y^+] \geq \tau$ , where  $\mathcal{S}$  is the softmax function.<sup>2</sup>

<sup>2</sup>For detailed background information on gradient-based counterfactual search and convergence see ?@sec-app-ce.

173 To train models with high explainability as defined in Definition 3.1, we propose to leverage counterfactuals in the  
 174 following objective:

$$\min_{\theta} \text{yloss}(\mathbf{M}_{\theta}(\mathbf{x}), \mathbf{y}) + \lambda_{\text{div}} \text{div}(\mathbf{x}, \mathbf{x}'_T, y; \theta) + \lambda_{\text{adv}} \text{advloss}(\mathbf{M}_{\theta}(\mathbf{x}'_{t \leq T}), \mathbf{y}) \quad (1)$$

175 where  $\text{yloss}(\cdot)$  is any conventional classification loss that induces discriminative performance (e.g., cross-entropy).  
 176 The two additional components in Equation 1 are explained in more detail below. For now, they can be sufficiently de-  
 177 scribed as inducing explainability directly and indirectly by penalizing: (1) the contrastive divergence,  $\text{div}(\cdot)$ , between  
 178 mature counterfactuals  $\mathbf{x}'_T$  and observed samples  $x$  and, (2) the adversarial loss,  $\text{advloss}(\cdot)$ , with respect to nascent  
 179 counterfactuals  $\mathbf{x}'_{t \leq T}$ . The tradeoff between the different components can be governed by adjusting the strengths of  
 180 the penalties  $\lambda_{\text{div}}$  and  $\lambda_{\text{adv}}$ .

### 181 3.1.1 Directly Inducing Explainability through Contrastive Divergence

182 Grathwohl et al. (2020) observe that any classifier can be re-interpreted as a joint energy-based model (JEM) that  
 183 learns to discriminate output classes conditional on the observed (training) samples from  $p(\mathbf{x})$  and the generated  
 184 samples from  $p_{\theta}(\mathbf{x})$ . They show that JEMs can be trained to perform well at both tasks by directly maximizing the  
 185 joint log-likelihood factorized as  $\log p_{\theta}(\mathbf{x}, \mathbf{y}) = \log p_{\theta}(\mathbf{y}|\mathbf{x}) + \log p_{\theta}(\mathbf{x})$ . The first factor can be optimized using  
 186 conventional cross-entropy as in Equation 1. Then, to optimize  $\log p_{\theta}(\mathbf{x})$  Grathwohl et al. (2020) minimize the  
 187 contrastive divergence between these observed samples from  $p(\mathbf{x})$  and generated samples from  $p_{\theta}(\mathbf{x})$ .

188 A key empirical finding in Altmeyer et al. (2024) was that JEMs tend to do well with respect to the plausibility ob-  
 189 jective in Definition 3.1. If we consider samples drawn from  $p_{\theta}(\mathbf{x})$  as counterfactuals, this is an expected finding,  
 190 because the JEM objective effectively minimizes the divergence between the conditional posterior and  $p(\mathbf{x}|y^+)$ . To  
 191 generate samples, Grathwohl et al. (2020) rely on Stochastic Gradient Langevin Dynamics (SGLD) using an uninfor-  
 192 mative prior for initialization. This is where we depart from their methodology: instead of SGLD, we propose to use  
 193 counterfactual explainers to generate counterfactuals of observed training samples. Specifically, we have:

$$\text{div}(\mathbf{x}, \mathbf{x}'_T, y; \theta) = \mathcal{E}_{\theta}(\mathbf{x}, y) - \mathcal{E}_{\theta}(\mathbf{x}'_T, y) \quad (2)$$

194 where  $\mathcal{E}_{\theta}(\cdot)$  denotes the energy function. In particular, we set  $\mathcal{E}_{\theta}(\mathbf{x}, y) = -\mathbf{M}_{\theta}(\mathbf{x}^+)[y^+]$  where  $y^+$  denotes the index  
 195 of the randomly drawn target class,  $y^+ \sim p(y)$ , and  $\mathbf{x}^+$  denotes an observed data point sampled from target domain:  
 196  $\mathbf{X}^+ = \{\mathbf{x} : y = y^+\}$ . Conditional on the target class  $y^+$ ,  $\mathbf{x}'_T$  denotes a mature counterfactual for a randomly sampled  
 197 factual from a non-target class generated through a gradient-based counterfactual generator for at most  $T$  iterations.  
 198 We define mature counterfactuals as those that have either exhausted  $T$  or reached convergence in terms of the pre-  
 199 determined decision threshold earlier.

200 Intuitively, the gradient of Equation 2 decreases the energy of observed training samples (positive samples) while at  
 201 same time increasing the energy of counterfactuals (negative samples) (Du and Mordatch 2020). As the generated  
 202 counterfactuals get more plausible (Definition 3.1) over the course of training, these two opposing effects gradually  
 203 balance each out (Lippe 2024).

204 The departure from SGLD allows us to tap into the vast repertoire of explainers that have been proposed in the literature  
 205 to meet different desiderata. Typically, these methods facilitate the imposition of domain and mutability constraints,  
 206 for example. In principle, any existing approach for generating counterfactual explanations is viable, so long as it does  
 207 not violate the faithfulness condition. Like JEMs (Murphy 2022), counterfactual training can be considered as a form  
 208 of contrastive representation learning.

### 209 3.1.2 Indirectly Inducing Explainability through Adversarial Robustness

210 Based on our analysis in Section 2, counterfactuals  $\mathbf{x}'$  can be repurposed as additional training samples (Luu and Inoue  
 211 2023; Balashankar et al. 2023) or adversarial examples (Freiesleben 2022; Pawelczyk et al. 2022). This leaves some  
 212 flexibility with respect to the exact choice for  $\text{advloss}(\cdot)$  in Equation 1. An intuitive functional form to use, though  
 213 likely not the only reasonable choice, is inspired by adversarial training:

$$\begin{aligned} \text{advloss}(\mathbf{M}_{\theta}(\mathbf{x}'_{t \leq T}), \mathbf{y}; \varepsilon) &= \text{yloss}(\mathbf{M}_{\theta}(\mathbf{x}'_{t_{\varepsilon}}), \mathbf{y}) \\ t_{\varepsilon} &= \max_t \{t : \|\Delta_t\|_{\infty} < \varepsilon\} \end{aligned} \quad (3)$$

214 Under this choice, we consider nascent counterfactuals  $\mathbf{x}'_{t \leq T}$  as adversarial examples as long as the magnitude of the  
 215 perturbation to any individual feature is at most  $\varepsilon$ . This is closely aligned with Szegedy et al. (2013), who define an  
 216 adversarial attack as an “imperceptible non-random perturbation”. Thus, we choose to work with a different distinction

217 between CE and AE than Freiesleben (2022), who considers misclassification as the key distinguishing feature of AE.  
 218 One of the key observations in this work is that we can leverage counterfactual explanations during training and get  
 219 adversarial examples, essentially for free.

220 **3.2 Encoding Actionability Constraints**

221 Many existing counterfactual explainers support domain and mutability constraints out-of-the-box. In fact, both types  
 222 of constraints can be implemented for any counterfactual explainer that relies on gradient descent in the feature space  
 223 for optimization (Altmeyer, van Deursen, and Liem 2023). In this context, domain constraints can be imposed by  
 224 simply projecting counterfactuals back to the specified domain, if the previous gradient step resulted in updated feature  
 225 values that were out-of-domain. Mutability constraints can similarly be enforced by setting partial derivatives to zero  
 226 to ensure that features are only mutated in the allowed direction, if at all.

227 Since actionability constraints are binding at test time, we should also impose them when generating  $\mathbf{x}'$  during each  
 228 training iteration to align model representations with user requirements. Through their effect on  $\mathbf{x}'$ , both types of  
 229 constraints influence model outcomes through Equation 2. Here it is crucial that we avoid penalizing implausibility  
 230 that arises due to mutability constraints. For any mutability-constrained feature  $d$  this can be achieved by enforcing  
 231  $\mathbf{x}[d] - \mathbf{x}'[d] := 0$  whenever perturbing  $\mathbf{x}'[d]$  in the direction of  $\mathbf{x}[d]$  would violate mutability constraints. Specifically,  
 232 we set  $\mathbf{x}[d] := \mathbf{x}'[d]$  if:

- 233    1. Feature  $d$  is strictly immutable in practice.  
 234    2. We have  $\mathbf{x}[d] > \mathbf{x}'[d]$  but feature  $d$  can only be decreased in practice.  
 235    3. We have  $\mathbf{x}[d] < \mathbf{x}'[d]$  but feature  $d$  can only be increased in practice.

236 From a Bayesian perspective, setting  $\mathbf{x}[d] := \mathbf{x}'[d]$  can be understood as assuming a point mass prior for  $p(\mathbf{x})$  with  
 237 respect to feature  $d$ . Intuitively, we think of this simply in terms ignoring implausibility costs with respect to immutable  
 238 features, which effectively forces the model to instead seek plausibility with respect to the remaining features. This  
 239 in turn results in lower overall sensitivity to immutable features, which we demonstrate empirically for different  
 240 classifiers in Section 4. Under certain conditions, this results holds theoretically:<sup>3</sup>

241 **Proposition 3.1** (Protecting Immutable Features). *Let  $f_\theta(\mathbf{x}) = \mathcal{S}(\mathbf{M}_\theta(\mathbf{x})) = \mathcal{S}(\Theta\mathbf{x})$  denote a linear classifier with  
 242 softmax activation  $\mathcal{S}$  (i.e., multinomial logistic regression) where  $y \in \{1, \dots, K\} = \mathcal{K}$  and  $\mathbf{x} \in \mathbb{R}^D$ . If we assume  
 243 multivariate Gaussian class densities with common diagonal covariance matrix  $\Sigma_k = \Sigma$  for all  $k \in \mathcal{K}$ , then protecting  
 244 an immutable feature from the contrastive divergence penalty (Equation 2) will result in lower classifier sensitivity to  
 245 that feature relative to the remaining features, provided that at least one of those is discriminative and mutable.*

246 It is worth highlighting that Proposition 3.1 assumes independence of features. This raises a valid concern about the  
 247 effect of protecting immutable features in the presence of proxy features that remain unprotected. We discuss this  
 248 limitation in Section 5.

249 **3.3 Illustration**

250 To better convey the intuition underlying our proposed method, we illustrate different model outcomes in Example 3.1.

251 **Example 3.1** (Prediction of Consumer Credit Default). Suppose we are interested in predicting the likelihood that  
 252 loan applicants default on their credit. We have access to historical data on previous loan takers comprised of a binary  
 253 outcome variable ( $y \in \{1 = \text{default}, 2 = \text{no default}\}$ ) two input features: (1) the subjects' *age*, which we define as  
 254 immutable, and (2) the subjects' existing level of *debt*, which we define as mutable.

255 We have simulated this scenario using synthetic data with independent features and Gaussian class-conditional densities  
 256 in Figure 1. The four panels in Figure 1 show the outcomes for different training procedures using the same model  
 257 architecture each time (a linear classifier). In each case, we show the linear decision boundary (green) and the training  
 258 data colored according to their ground-truth label: orange points belong to the target class,  $y^+ = 2$ , blue points belong  
 259 to the non-target class,  $y^- = 1$ . Stars indicate counterfactuals in the target class generated at test time using generic  
 260 gradient descent until convergence.

261 In panel (a), we have trained our model conventionally, and we do not impose mutability constraints at test time. The  
 262 generated counterfactuals are all valid, but not plausible: they are clearly distinguishable from the ground-truth data. In  
 263 panel (b), we have trained our model with counterfactual training, once again not imposing mutability constraints at test  
 264 time. We observe that the counterfactuals are clearly plausible, therefore meeting the first objective of Definition 3.1.

265 In panel (c), we have used conventional training again, this time imposing the mutability constraint on *age* at test time.  
 266 Counterfactuals are valid but involve some substantial reductions in *debt* for some individuals (very young applicants).

---

<sup>3</sup>For the proof, see the supplementary appendix.

267 By comparison, counterfactual paths are shorter on average in panel (d), where we have used counterfactual training  
 268 and protected immutable features as described in Section 3.2. In particular, we observe that due to the classifier's  
 269 lower sensitivity to *age*, recourse recommendations with respect to *debt* are much more homogenous, in that they do  
 270 not disproportionately punish younger individuals. The counterfactuals are also plausible with respect to the mutable  
 271 feature. Thus, we consider the model in panel (d) as the most explainable according to Definition 3.1.

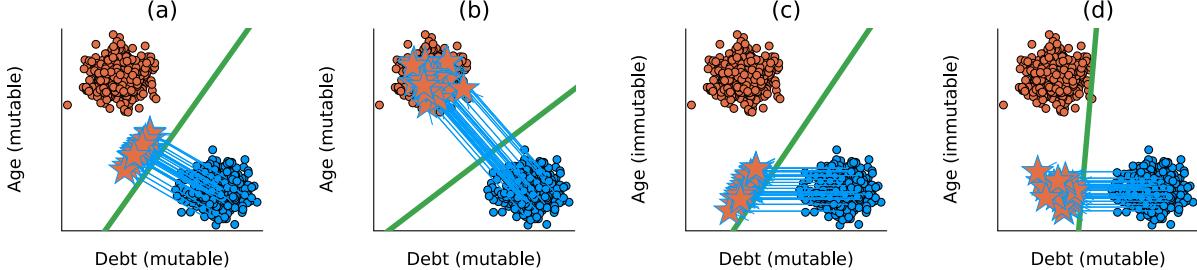


Figure 1: Visual illustration of how counterfactual training improves explainability. See Example 3.1 for details.

## 272 4 Experiments

273 In this section, we present experiments that we have conducted in order to answer the following research questions:

274 **Research Question 4.1** (Plausibility). *Does our proposed counterfactual training objective (Equation 1) induce mod-  
 275 els to learn plausible explanations?*

276 **Research Question 4.2** (Actionability). *Does our proposed counterfactual training objective (Equation 1) yield more  
 277 favorable algorithmic recourse outcomes in the presence of actionability constraints?*

278 Beyond this, we are also interested in understanding how robust our answers to RQ 4.1 and RQ 4.2 are:

279 **Research Question 4.3** (Hyperparameters). *What are the effects of different hyperparameter choices with respect to  
 280 Equation 1?*

### 281 4.1 Experimental Setup

#### 282 4.1.1 Evaluation

283 Our key outcome of interest is how well models perform with respect to explainability (Definition 3.1): to this end, we  
 284 focus primarily on the plausibility and cost of faithfully generated counterfactuals at test time. To measure the cost of  
 285 counterfactuals, we follow the standard convention of using distances ( $\ell_1$ -norm) between factuals and counterfactuals  
 286 as a proxy. For plausibility, we assess how similar counterfactuals are to observed samples in the target domain. We  
 287 rely on the distance-based metric used by Altmeyer et al. (2024),

$$\text{implaus}_{\text{dist}}(\mathbf{x}', \mathbf{X}^+) = \frac{1}{|\mathbf{X}^+|} \sum_{\mathbf{x} \in \mathbf{X}^+} \text{dist}(\mathbf{x}', \mathbf{x}) \quad (4)$$

288 and introduce a novel divergence metric,

$$\text{implaus}_{\text{div}}(\mathbf{X}', \mathbf{X}^+) = \text{MMD}(\mathbf{X}', \mathbf{X}^+) \quad (5)$$

289 where  $\mathbf{X}'$  denotes a set of multiple counterfactuals and  $\text{MMD}(\cdot)$  is an unbiased estimate of the squared population  
 290 maximum mean discrepancy (Gretton et al. 2012). The metric in Equation 5 is equal to zero iff  $\mathbf{X}' = \mathbf{X}^+$ .

291 In addition to cost and plausibility, we also compute other standard metrics to evaluate counterfactuals at test time in-  
 292 cluding validity and redundancy. Finally, we also assess the predictive performance of models using standard metrics.

293 We run the experiments with three CE generators: *Generic* of Wachter, Mittelstadt, and Russell (2017) as a simple  
 294 baseline approach, *REVISE* (Joshi et al. 2019) that aims to generate plausible counterfactuals using a surrogate Vari-  
 295 ational Autoencoder (VAE), and *ECCo*—the generator of Altmeyer et al. (2023) but without the conformal prediction  
 296 component—as a method that directly targets both faithfulness and plausibility of the CEs.

297 **4.2 Experimental Results**298 **4.2.1 Plausibility**299 **4.2.2 Actionability**300 **4.2.3 Impact of hyperparameter settings**

301 We extensively test the impact of three types of hyperparameters on the proposed training regime. Our complete results  
 302 are available in the technical appendix; this section focuses on the main findings.

303 **Hyperparameters of the CE generators.** First, we observe that CT is highly sensitive to hyperparameter settings but  
 304 (a) there are manageable patterns and (b) we can typically identify settings that improve either plausibility or cost, and  
 305 commonly both of them at the same time. Second, we note that the choice of a CE generator has a major impact on  
 306 the results. For example, *REVISE* tends to perform the worst, most likely because it attempts to explain the decisions  
 307 of a VAE that is an imperfect surrogate of the original model. Third, increasing  $T$ , the maximum number of steps,  
 308 generally yields better outcomes because more CEs can mature in any iteration. Fourth, the impact of  $\tau$ , the required  
 309 decision threshold is more difficult to predict. On “harder” datasets it may be difficult to satisfy high  $\tau$  for any given  
 310 sample (i.e., also factuals) and so increasing this threshold does not seem to correlate with better outcomes.

311 **Hyperparameters for penalties** We find that the strength of the energy regularization,  $\lambda_{\text{reg}}$  is highly impactful; energy  
 312 must be sufficiently regularized to avoid poor performance in terms of decreased plausibility and increased costs. The  
 313 sensitivity with respect to  $\lambda_{\text{div}}$  and  $\lambda_{\text{adv}}$  is much less evident. While high values of  $\lambda_{\text{reg}}$  may increase the variability in  
 314 outcomes when combined with high values for Equation 1 penalties, this effect is not very pronounced.

315 **Other hyperparameters.** We observe that the effectiveness and stability of CT is positively associated with the number  
 316 of counterfactuals generated during each training epoch. We also confirm that a higher number of training epochs is  
 317 beneficial. Interestingly, we find that it is not necessary to employ CT during the entire training phase to achieve the  
 318 desired improvements in explainability. We have tested training models conventionally during the first half of training  
 319 before switching to CT after this initial “burn-in” period and observed positive results. Put differently, CT may be a  
 320 way to improve the explainability of trained models in a fine-tuning manner.

321 **5 Discussion**322 **5.1 Approach/Future Directions**

- 323 1. Limited to classification models.
- 324 2. Training instabilities.
- 325 3. Hyperparameter sensitivity -> can we do better than grid search? (Bayes opt, ...)

326 **5.2 Limitations**

- 327 3. Proxy attributes of immutable features.
- 328 4. Increased training time.
- 329 5. Fairness and caveats (aware it's not a classical approach in this context, but there is a clear link).

330 **6 Conclusion**331 **References**

- 332 Abbasnejad, Ehsan, Damien Teney, Amin Parvaneh, Javen Shi, and Anton van den Hengel. 2020. “Counterfactual  
 333 Vision and Language Learning.” In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition*  
 334 (*CVPR*), 10041–51. <https://doi.org/10.1109/CVPR42600.2020.01006>.
- 335 Altmeyer, Patrick, Mojtaba Farmanbar, Arie van Deursen, and Cynthia C. S. Liem. 2023. “Faithful Model Explanations  
 336 Through Energy-Constrained Conformal Counterfactuals.” <https://arxiv.org/abs/2312.10648>.
- 337 Altmeyer, Patrick, Mojtaba Farmanbar, Arie van Deursen, and Cynthia CS Liem. 2024. “Faithful Model Explanations  
 338 Through Energy-Constrained Conformal Counterfactuals.” In *Proceedings of the AAAI Conference on Artificial*  
 339 *Intelligence*, 38:10829–37. 10.
- 340 Altmeyer, Patrick, Arie van Deursen, and Cynthia C. S. Liem. 2023. “Explaining Black-Box Models Through Coun-  
 341 terfactuals.” In *Proceedings of the JuliaCon Conferences*, 1:130. 1.
- 342 Augustin, Maximilian, Alexander Meinke, and Matthias Hein. 2020. “Adversarial Robustness on in-and Out-  
 343 Distribution Improves Explainability.” In *European Conference on Computer Vision*, 228–45. Springer.
- 344 Balashankar, Ananth, Xuezhi Wang, Yao Qin, Ben Packer, Nithum Thain, Ed Chi, Jilin Chen, and Alex Beutel. 2023.  
 345 “Improving Classifier Robustness Through Active Generative Counterfactual Data Augmentation.” In *Findings of*  
 346 *the Association for Computational Linguistics: EMNLP 2023*, 127–39.

- 347 Du, Yilun, and Igor Mordatch. 2020. “Implicit Generation and Generalization in Energy-Based Models.” <https://arxiv.org/abs/1903.08689>.
- 348 Frankle, Jonathan, and Michael Carbin. 2019. “The Lottery Ticket Hypothesis: Finding Sparse, Trainable Neural Net-  
349 works.” In *International Conference on Learning Representations*. <https://openreview.net/forum?id=rJl-b3RcF7>.
- 350 Freiesleben, Timo. 2022. “The Intriguing Relation Between Counterfactual Explanations and Adversarial Examples.”  
351 *Minds and Machines* 32 (1): 77–109.
- 352 Goodfellow, Ian J, Jonathon Shlens, and Christian Szegedy. 2014. “Explaining and Harnessing Adversarial Examples.”  
353 <https://arxiv.org/abs/1412.6572>.
- 354 Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. 2016. *Deep Learning*. MIT Press.
- 355 Grathwohl, Will, Kuan-Chieh Wang, Joern-Henrik Jacobsen, David Duvenaud, Mohammad Norouzi, and Kevin Swer-  
356 sky. 2020. “Your Classifier Is Secretly an Energy Based Model and You Should Treat It Like One.” In *International  
357 Conference on Learning Representations*.
- 358 Gretton, Arthur, Karsten M Borgwardt, Malte J Rasch, Bernhard Schölkopf, and Alexander Smola. 2012. “A Kernel  
359 Two-Sample Test.” *The Journal of Machine Learning Research* 13 (1): 723–73.
- 360 Guidotti, Riccardo. 2022. “Counterfactual Explanations and How to Find Them: Literature Review and Benchmark-  
361 ing.” *Data Mining and Knowledge Discovery*, 1–55.
- 362 Guo, Hangzhi, Thanh H. Nguyen, and Amulya Yadav. 2023. “CounterNet: End-to-End Training of Prediction Aware  
363 Counterfactual Explanations.” In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery  
364 and Data Mining*, 577–89. KDD ’23. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3580305.3599290>.
- 365 Joshi, Shalmali, Oluwasanmi Koyejo, Warut Vigitbenjaronk, Been Kim, and Joydeep Ghosh. 2019. “Towards Realistic  
366 Individual Recourse and Actionable Explanations in Black-Box Decision Making Systems.” <https://arxiv.org/abs/1907.09615>.
- 367 Kolter, Zico. 2023. “Keynote Addresses: SaTML 2023 .” In *2023 IEEE Conference on Secure and Trustworthy  
368 Machine Learning (SaTML)*, xvi–. Los Alamitos, CA, USA: IEEE Computer Society. <https://doi.org/10.1109/SaTML54575.2023.00009>.
- 369 Lakshminarayanan, Balaji, Alexander Pritzel, and Charles Blundell. 2017. “Simple and Scalable Predictive Uncer-  
370 tainty Estimation Using Deep Ensembles.” *Advances in Neural Information Processing Systems* 30.
- 371 Lippe, Phillip. 2024. “UvA Deep Learning Tutorials.” <https://uvadlc-notebooks.readthedocs.io/en/latest/>.
- 372 Luu, Hoai Linh, and Naoya Inoue. 2023. “Counterfactual Adversarial Training for Improving Robustness of Pre-  
373 Trained Language Models.” In *Proceedings of the 37th Pacific Asia Conference on Language, Information and  
374 Computation*, 881–88.
- 375 McGregor, Sean. 2021. “Preventing repeated real world AI failures by cataloging incidents: The AI incident database.”  
376 In *Proceedings of the AAAI Conference on Artificial Intelligence*, 35:15458–63. 17.
- 377 Morcos, Ari S., Haonan Yu, Michela Paganini, and Yuandong Tian. 2019. “One Ticket to Win Them All: Gener-  
378 alizing Lottery Ticket Initializations Across Datasets and Optimizers.” In *Proceedings of the 33rd International  
379 Conference on Neural Information Processing Systems*. Red Hook, NY, USA: Curran Associates Inc.
- 380 Murphy, Kevin P. 2022. *Probabilistic Machine Learning: An Introduction*. MIT Press.
- 381 O’Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*.  
382 Crown.
- 383 Pawelczyk, Martin, Chirag Agarwal, Shalmali Joshi, Sohini Upadhyay, and Himabindu Lakkaraju. 2022. “Exploring  
384 Counterfactual Explanations Through the Lens of Adversarial Examples: A Theoretical and Empirical Analysis.”  
385 In *Proceedings of the 25th International Conference on Artificial Intelligence and Statistics*, edited by Gustau  
386 Camps-Valls, Francisco J. R. Ruiz, and Isabel Valera, 151:4574–94. Proceedings of Machine Learning Research.  
387 PMLR. <https://proceedings.mlr.press/v151/pawelczyk22a.html>.
- 388 Poyiadzi, Rafael, Kacper Sokol, Raul Santos-Rodriguez, Tijl De Bie, and Peter Flach. 2020. “FACE: Feasible and  
389 Actionable Counterfactual Explanations.” In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*,  
390 344–50.
- 391 Ross, Alexis, Himabindu Lakkaraju, and Osbert Bastani. 2024. “Learning Models for Actionable Recourse.” In  
392 *Proceedings of the 35th International Conference on Neural Information Processing Systems*. NIPS ’21. Red  
393 Hook, NY, USA: Curran Associates Inc.
- 394 Sauer, Axel, and Andreas Geiger. 2021. “Counterfactual Generative Networks.” <https://arxiv.org/abs/2101.06046>.
- 395 Schut, Lisa, Oscar Key, Rory Mc Grath, Luca Costabello, Bogdan Sacaleanu, Yarin Gal, et al. 2021. “Generating  
396 Interpretable Counterfactual Explanations By Implicit Minimisation of Epistemic and Aleatoric Uncertainties.” In  
397 *International Conference on Artificial Intelligence and Statistics*, 1756–64. PMLR.
- 398 Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus.  
399 2013. “Intriguing Properties of Neural Networks.” <https://arxiv.org/abs/1312.6199>.

- 404 Tenev, Damien, Ehsan Abbasnedjad, and Anton van den Hengel. 2020. “Learning What Makes a Difference from  
 405 Counterfactual Examples and Gradient Supervision.” In *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part x 16*, 580–99. Springer.  
 406
- 407 Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2017. “Counterfactual Explanations Without Opening the Black  
 408 Box: Automated Decisions and the GDPR.” *Harv. JL & Tech.* 31: 841. <https://doi.org/10.2139/ssrn.3063289>.  
 409
- 410 Wilson, Andrew Gordon. 2020. “The Case for Bayesian Deep Learning.” <https://arxiv.org/abs/2001.10995>.  
 411
- 412 Wu, Tongshuang, Marco Tulio Ribeiro, Jeffrey Heer, and Daniel Weld. 2021. “Polyjuice: Generating Counterfactuals  
 413 for Explaining, Evaluating, and Improving Models.” In *Proceedings of the 59th Annual Meeting of the Association  
 414 for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing  
 (Volume 1: Long Papers)*, edited by Chengqing Zong, Fei Xia, Wenjie Li, and Roberto Navigli, 6707–23. Online:  
 415 Association for Computational Linguistics. <https://doi.org/10.18653/v1/2021.acl-long.523>.  
 416
- 417 Zhang, Chiyuan, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals. 2021. “Understanding Deep  
 417 Learning (Still) Requires Rethinking Generalization.” *Commun. ACM* 64 (3): 107–15. <https://doi.org/10.1145/3446776>.