
Preserving Causal Constraints in Counterfactual Explanations for Machine Learning Classifiers

Divyat Mahajan

Microsoft Research
Bangalore, India

divyatmahajan@gmail.com

Chenhao Tan

University of Colorado Boulder
Boulder, USA

chenhao@chenhaot.com

Amit Sharma

Microsoft Research
Bangalore, India

amshar@microsoft.com

Abstract

To construct interpretable explanations that are consistent with the original ML model, *counterfactual* examples—showing how the model’s output changes with small perturbations to the input—have been proposed. This paper extends the work in counterfactual explanations by addressing the challenge of *feasibility* of such examples. For explanations of ML models in critical domains such as healthcare and finance, counterfactual examples are useful for an end-user only to the extent that perturbation of feature inputs is feasible in the real world. We formulate the problem of feasibility as preserving causal relationships among input features and present a method that uses (partial) structural causal models to generate actionable counterfactuals. When feasibility constraints cannot be easily expressed, we consider an alternative mechanism where people can label generated CF examples on feasibility: whether it is feasible to intervene and realize the candidate CF example from the original input. To learn from this labelled feasibility data, we propose a modified variational auto encoder loss for generating CF examples that optimizes for feasibility as people interact with its output. Our experiments on Bayesian networks and the widely used “Adult-Income” dataset show that our proposed methods can generate counterfactual explanations that better satisfy feasibility constraints than existing methods. Code repository can be accessed here: <https://github.com/divyat09/cf-feasibility>

1 Introduction

Local explanations for a machine learning model are important for people to interpret its output, especially in critical decision-making scenarios such as healthcare, governance, and finance. Techniques for explaining an ML model often involve a simpler surrogate model that yields interpretable information, such as feature importance scores [1]. However, these techniques suffer from an inherent fidelity-interpretability tradeoff due to their use of a simpler model for generating explanations. Highly interpretable explanations may end up approximating too much and be inconsistent with the original ML model (low fidelity), while high fidelity explanations may be as complex as the original ML model and thus less interpretable.

Counterfactual explanations [2] have been proposed as an alternative that are always consistent with the original ML model and arguably may also be interpretable. Counterfactual (CF) explanations present the perturbations in the original input features that could have led to a change in the prediction of the model. For example, consider a person whose loan application has been rejected by an ML classifier. For this person, a CF explanation provides what-if scenarios wherein they would have their loan approved, e.g., “*your loan would have been approved if your income was \$10000 more*”. Since the goal is to generate perturbations of an input that lead to a different outcome from the ML model, CF explanation has parallels with adversarial examples [3].

However, one of the biggest challenges with counterfactual explanation is to generate examples that are *feasible* in the real world. Continuing with the loan example, the counterfactual changes in the input should follow some natural laws (e.g., age cannot decrease) and knowledge about interactions between features (e.g., changing education level without changing age is impossible). Recent work [4, 5, 6] tries to address feasibility using statistical constraints during generation of CFs, such as encouraging CF examples that are more likely given the training data.

Our main contribution is to show that feasibility is fundamentally a causal concept, and cannot be addressed with statistical constraints alone. We formally define feasibility for a CF example based on an underlying structural causal model between input features: a CF example is feasible if the changes satisfy constraints entailed by the causal model. To bring out the difference with statistical constraints, consider a CF example that recommends “increase education level to Masters” without changing the age of a person. Such a CF example is infeasible but will satisfy constraints from past work, including change in only actionable features [4], and being likely given the observed data [5] (it may be likely to observe others with the same age and a Masters degree). Similarly an infeasible CF example that recommends “decrease age by 3 years” satisfies the constraint from [6] that intermediate CFs on the path (e.g., people with same features but age reduced by 1 and 2 years) are likely, but is impossible to act upon. We call this *global* feasibility that must be satisfied by all counterfactual examples. We also define *local* feasibility that depends on an end-user’s context or preferences.

To generate feasible CF explanations, we propose a *causal proximity* regularizer that can be added to any CF generation method instead of the standard proximity measure based on ℓ_1 or ℓ_2 distance [2]. The proposed proximity loss is based on causal relationships between features, as modeled by a structural causal model (SCM) of input features. In practice, we show how the loss can be derived from a partial SCM, or common unary and binary constraints such as monotonic change between features. In many cases, however, it is not possible to express feasibility with simple constraints. Therefore, we propose a second method that learns feasibility constraints from users’ binary feedback on its generated counterfactuals. Our method modifies the standard variational autoencoder’s objective to adapt it for generating CFs while encouraging feasibility as defined by users’ labels.

Results on Adult-Income and synthetic Bayesian network datasets show that our proposed methods can generate counterfactual examples that are more feasible than models that do not include causal assumptions or user feedback. Further, our novel generative model is much faster than existing approaches to generate CFs. To summarize, our contributions include:

- We provide a causal view of the feasibility of CF examples that includes many kinds of constraints not considered in prior work.
- To address feasibility, we propose a causal proximity regularizer based on constraints derived from an SCM, that can be applied to any method for generating CF examples.
- When feasibility constraints are not available, we propose a VAE-based generative model that can learn feasibility constraints from user feedback.

2 A Causal View of Feasibility of CF Explanations

Throughout, we assume a machine learning classifier, $h : \mathcal{X} \rightarrow \mathcal{Y}$ where $\mathbf{x} \in \mathcal{X}$ are the features and $y \in \mathcal{Y}$ is a categorical output. A *valid* counterfactual example for an input \mathbf{x} and outcome y is one that changes the outcome of h to the desired outcome y' [7]. Counterfactual generation is usually framed as solving an optimization problem that searches in the feature space to find perturbations that are proximal (close to the original input) but lead to a different output class from the machine learning model. [2] provide the following optimization to generate a CF example \mathbf{x}^{cf} for an input instance \mathbf{x} given a ML model h , where the target class is y' :

$$\operatorname{argmin}_{\mathbf{x}^{cf}} \text{Loss}(h(\mathbf{x}^{cf}), y') + \text{Dist}(\mathbf{x}, \mathbf{x}^{cf}). \quad (1)$$

Loss refers to a classification loss (such as cross-entropy) and Dist refers to a distance metric (such as ℓ_2 distance). That is, we seek to generate counterfactual explanations that belong to a target class y' while still remaining proximal to the original input.

Note that under this formulation, there are two limitations: 1) features of the input \mathbf{x} may be changed independently to construct \mathbf{x}^{cf} , and 2) a new optimization problem needs to be solved for each

new input. For the first, we propose a definition for incorporating feasibility below. For the second, Section 3.1 provides a generative model that once trained, can easily generate multiple new CFs.

2.1 Global Feasibility

Definition 2.1. Causal Model [8]. A causal model is a triplet $M = \langle U, V, F \rangle$ such that U is a set of exogenous variables, V is a set of endogenous variables that are determined by variables inside the model, and F is a set of functions that determine the value of each $v_i \in V$ (up to some independent noise) based on values of $U_i \cup Pa_i$ where $U_i \subseteq U$ and $Pa_i \subseteq V \setminus v_i$.

Definition 2.2. Global Feasibility. Let $\langle x_i, y_i \rangle$ be the input features and the predicted outcome from h , and let y' be the desired output class. Let $M = \langle U, V, F \rangle$ be a causal model over \mathcal{X} such that each feature is in $U \cup V$. Then, a counterfactual example $\langle x^{cf}, y^{cf} \rangle$ is globally feasible if it is valid ($y^{cf} = y'$), the change from x_i to x^{cf} satisfies all constraints entailed by the causal model, and all exogenous variables $x^{exog} = U$ lie within the input domain.

For example, a CF example that changes an individual’s age to 300 is infeasible since it violates the limits of the input domain of the age feature. In general, such constraints relating to the input domain may be learned from an i.i.d. sample of data by estimating the joint distribution of features. E.g., [5] use an auto-encoder loss-term to align CF examples to the data distribution.

In addition, however, a CF example that decreases age is infeasible since it violates the natural causal model/constraint that age can only increase with time. Such *causal constraints cannot be learned from data alone, and often need extra information* [8]. More complex causal constraints can be defined over pairs or multiple variables. For example, in the loan decision example from above, we can consider v_{p1} as *education-level* and v as *age*, and posit a causal relationship that increasing *education-level* needs years to complete and thus causes *age* to increase. That is, any counterfactual example that increases *education-level* without increasing *age* is infeasible, although a counterfactual example that increases *age* without changing *education-level* may still be feasible as we do not know the full set of causes that may increase *age*. While some of these feasibility constraints can be formulated in simple terms, causal relationships over multiple features can lead to complex constraints. As we show below, they can be defined formally using structural causal models, and implemented as constraints on how features can change (Section 2.4). Constraints from an SCM can also be probabilistic (e.g., increasing education level with a six-month increase in age is unlikely). We may define *degree of feasibility* as the joint probability of changes in selected features.

2.2 Local Feasibility

For a particular user, a globally feasible CF example may still be infeasible due to an end-user’s context or personal preferences. Thus, while global feasibility is a necessary condition for feasible CFs, we also need to define local feasibility.

Definition 2.3. Local Feasibility: A CF example is locally feasible for a user if it is globally feasible and satisfies user-level constraints.

For example, a user may find it difficult to change their city because of family constraints. Thus, a counterfactual example may be locally infeasible due to many user specific factors. Preserving global constraints entailed from a causal model provides necessary conditions for a feasible counterfactual, but customization may be needed for local feasibility.

2.3 A causal proximity loss for generating CF examples

We now define a feasibility-compatible notion of distance to constrain independent perturbations of features. We want the counterfactual to be proximal to the data sample not only based on the Euclidean distance between them, but also based on the causal relationships between features.

Suppose we are provided with the structural causal model [8] for the observed data, including the causal graph G over $U \cup V$ and the functional relationships between variables. V is the set of all endogenous nodes that have at least one parent in the graph. For exogenous variables U , we use the standard proximity loss (e.g., using the ℓ_1/ℓ_2 distance). For each endogenous node $v \in V$ that has at least one parent in the graph, we propose a new feasibility-compatible distance metric based on the

generating mechanism of v conditioned on its parents, i.e., $v = f(v_{p1}, \dots, v_{pk}) + \epsilon$ where v_p refers to parent nodes of v and ϵ denotes independent random noise. For each node $v \in V$,

$$\text{DistCausal}_v(x_v, x_v^{cf}) = \text{Dist}_v(x_v^{cf}, f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}))$$

where $f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}) = \mathbb{E}[x_v^{cf} | x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}]$. This distance metric (Fig. 1) indicates that the counterfactual value for the feature v should depend on the values of its parents in the counterfactual example. Once its parents' counterfactual values have been decided, its value should ideally be the one predicted by the SCM function f . Note that the distance metric does not compare to the original value x_v , as in the standard proximity loss from Equation 1. Having the standard proximity loss on the exogenous features and the causal proximity loss on all other features ensures that an ideal CF is close to the original input instance and also preserves the causal relationship between features.

Hence, the Dist term in the CF generation loss function (Eq. 1) can be modified to generate counterfactuals that preserve causal constraints, where U are the exogenous nodes (i.e., nodes without any parents in the causal graph) and V are the remaining features.

$$\text{DistCausal}(\mathbf{x}, \mathbf{x}^{cf}) = \sum_{u \in U} \text{Dist}_u(x_u^{cf}, x_u) + \sum_{v \in V} \text{DistCausal}_v(x_v, x_v^{cf})$$

Since knowing the full causal graph is often impractical, the above approach can also work whenever we have partial knowledge of the causal structure (e.g., some edges in the causal graph). From this partial causal knowledge, we construct a set of nodes V for which we know the generating mechanism for each node $v \in V$ conditioned on its parents and consider the rest of the variables in U . We refer to this approach as Model-based CF.

2.4 Building a feasibility-compatible CF explanation method

Our proposed proximity loss can be combined with any prior CF generation method, by replacing the proximity term: $\text{argmin}_{\mathbf{x}^{cf}} \text{Loss}(h(\mathbf{x}^{cf}), y') + \text{DistCausal}(\mathbf{x}, \mathbf{x}^{cf})$. However, in practice, the exact functional causal mechanism for a variable is often unknown. Therefore, we present a simple approximation of the above loss by directly optimizing for certain constraints based on domain knowledge. For example, one may know that Age of a person cannot decrease, or that Education-level shares a monotonic causal relationship with Age, without knowing the true functional form. Below we provide example loss terms for common unary and binary feasibility constraints.

Unary constraints. We consider unary constraints that stipulate whether a feature can increase or decrease and define a hinge loss on the feature of interest. As an example, for the case that a feature can only increase, the hinge loss would be as follows: $-\min(0, \mathbf{x}_v^{cf} - \mathbf{x}_v)$.

Binary constraints. Binary constraints capture the nature of causal relationship between two features. One of the most common are monotonic constraints, which we approximate by learning an appropriate linear model for each binary constraint. Let x_1 and x_2 be two features where x_1 causes x_2 and we have a monotonically increasing trend between them. We capture this monotonic trend by learning a linear model between x_1 and x_2 , under the constraint that the parameter that relates x_1 to x_2 should be positive (or negative depending on the nature of monotonicity). This can be learnt by minimizing the following loss function over training data: $+(x_{v_2} - \alpha - \beta x_{v_1}) - \min(0, \beta)$, where α and β are parameters that can be learned from training data. We refer to this approach as Model-approx CF.

3 Example-Based Generation of Feasible CF explanations

In most situations, however, it is difficult to express complex constraints involving multiple features as convex loss terms. A more practical setting is that a user may provide feedback on generated counterfactuals to say which ones are feasible, and the CF generation method should learn feasibility

constraints through this feedback. For this to work interactively with a user, we need a pre-trained CF generation method that can generate initial CFs for different inputs and then update its generation method in a fast manner. Past approaches [5, 7] to CF generation run a new optimization for each input and can be difficult to fine-tune online. We thus propose a model-based method, **Example-Based CF**. It includes a variational autoencoder (VAE) module that parameterizes generation of CFs, and a fine-tuning model that updates model parameters to support feasibility.

3.1 Base VAE generator for CF explanations

We define the CF objective as generating CF examples \mathbf{x}^{cf} as building a model that maximizes $\Pr(\mathbf{x}^{cf}|y', \mathbf{x})$ such that \mathbf{x}^{cf} belongs to class y' . Our approach is based on an encoder-decoder framework where the task of the encoder is to project input features to a suitable latent space and the task of the decoder is to generate a counterfactual from the latent representation given by the encoder. Analogous to a variational auto-encoder (VAE) [9], we first arrive at a latent representation \mathbf{z} for the input instance \mathbf{x} via the encoder $q(\mathbf{z}|\mathbf{x}, y')$ and then generate the corresponding counterfactual \mathbf{x}^{cf} via the decoder $p(\mathbf{x}^{cf}|\mathbf{z}, y')$. Following the construction in VAEs [9], we first derive the evidence lower bound (ELBO) for generating CF explanations.

Theorem 1. *The evidence lower bound to optimize the CF objective $\Pr(\mathbf{x}^{cf}|y', \mathbf{x})$ is:*

$$\ln \Pr(\mathbf{x}^{cf}|y', \mathbf{x}) \geq \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x}) - \text{KL}(Q(\mathbf{z}|\mathbf{x}, y')||P(\mathbf{z}|y', \mathbf{x})).$$

The proof is in the **Suppl. A**. The prior of the latent variable \mathbf{z} is modulated by y' and \mathbf{x} , but following [10], we simply use $p(\mathbf{z}|y', \mathbf{x}) \sim \mathcal{N}(\mu_{y'}, \sigma_{y'}^2)$, so the KL Divergence can be computed in closed form. $P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x})$ represents the probability of the output \mathbf{x}^{cf} given the desired class and latent variable \mathbf{z} . This can be empirically estimated by the ℓ_1/ℓ_2 loss or any general Distance metric between input \mathbf{x} and \mathbf{x}^{cf} . That is, without additional assumptions, we are assuming that probability $P(\mathbf{x}^{cf})$ is highest near \mathbf{x} . In addition, this probability expression is conditioned on y' , implying that \mathbf{x}^{cf} is valid only if belongs to y' class when applied with h . We thus use a classification loss (e.g., hinge-loss) between $h(\mathbf{x}^{cf})$ and y' , where y' represents the target class and β represents the margin where λ is a hyperparameter.

$$\mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x}) \approx \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} [\text{Dist}(\mathbf{x}, \mathbf{x}^{cf}) + \lambda \text{HingeLoss}(h(\mathbf{x}^{cf}), y', \beta)],$$

where the hinge loss function is defined over the softmax scores s_y for each class output of h : $\text{HingeLoss}(h(\mathbf{x}^{cf}), y', \beta) = \max\{\max_{y \neq y'}\{s_y(\mathbf{x}^{cf})\} - s_{y'}(\mathbf{x}^{cf})\}, -\beta\}$. The above Hinge Loss formulation encourages classifier's score on target class to be higher than any other class by at least a margin of β . To summarize, given the ML model h to be explained, we learn our proposed model by minimizing the following loss function (BaseGenCFLoss):

$$\mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} [\text{Dist}(\mathbf{x}, \mathbf{x}^{cf}) + \lambda \text{HingeLoss}(h(\mathbf{x}^{cf}), y', \beta)] + \text{KL}(Q(\mathbf{z}|\mathbf{x}, y')||P(\mathbf{z}|y', \mathbf{x})),$$

where y' is the target counterfactual class. Our loss formulation bears an intuitive resemblance with the standard counterfactual loss formulation (Eq. 1). $\text{HingeLoss}(h(\mathbf{x}^{cf}), y', \beta)$ helps us to generate valid counterfactuals with respect to the ML model h , and $\text{Distance}(\mathbf{x}, \mathbf{x}^{cf})$ helps us to generate counterfactuals that are close to the input feature. The additional third term in the loss function represents the KL divergence between the prior distribution $p(\mathbf{z}|y')$ and the latent space encoder $q(\mathbf{z}|\mathbf{x}, y')$, analogous to the loss term in a VAE [9]. Our encoder-decoder framework can be viewed as an adaptation of VAE for the task of generating counterfactuals. Typically, the Dist function can be defined as the ℓ_1 distance between the input \mathbf{x} and the counterfactual \mathbf{x}^{cf} : $\text{Dist}(\mathbf{x}, \mathbf{x}^{cf}) = \|\mathbf{x} - \mathbf{x}^{cf}\|_1$.

3.2 Learning feasibility constraints through user feedback

We consider the user as an Oracle that provides binary yes/no feedback on feasibility of a generated CF. Given any input pair $(\mathbf{x}, \mathbf{x}^{cf})$ the oracle outputs 1 if the CF example is feasible, otherwise it outputs 0. Hence, in order to generate feasible counterfactuals, our task is to maximize the Oracle

Algorithm 1: Example-Based CF

Input: Training data $(\mathbf{x}, y)_{j=1}^n$

Output: Counterfactuals \mathbf{x}^{cf}

Base training phase: Learn a base VAE and generate query CFs $(\mathbf{x}_i, \mathbf{x}'_i)$ to be labelled for feasibility.

Feasibility learning phase: Given labelled queries $(\mathbf{x}_i, \mathbf{x}'_i, o_i)_{i=1}^q$, fine-tune the trained VAE with the following loss where λ is a hyperparameter trading off between validity/proximity and feasibility:

$$\min \sum_{i=1}^q [\text{BaseGenCFLoss}(\mathbf{x}_i, \mathbf{x}'_i) + \lambda_o ||o_i - \text{sim}(\mathbf{x}_i^{cf}, \mathbf{x}'_i)||_2^2].$$

score with as few queries to the Oracle as possible. Consider a dataset $(\mathbf{x}_i, \mathbf{x}'_i, o_i)_{i=1}^q$ where \mathbf{x}'_i is the CF example for \mathbf{x}_i and o_i is the output of the oracle.

For any new \mathbf{x} , ideally the output \mathbf{x}^{cf} of our model should have a high score. Thus the \mathbf{x}^{cf} should be similar to the feasible CFs and dissimilar to infeasible CFs in the query set. We write the similarity of \mathbf{x}^{cf} generated by our model and a query $(\mathbf{x}_i, \mathbf{x}'_i)$ as: $\text{sim}(\mathbf{x}_i^{cf}, \mathbf{x}'_i) = \exp(-(\mathbf{x}'_i - \mathbf{x}_i^{cf})^T (\mathbf{x}'_i - \mathbf{x}_i^{cf}))$ where \mathbf{x}'_i is the output of the VAE with input \mathbf{x}_i . The similarity should be higher when $o_i = 1$ and lower when $o_i = 0$, leading to the loss: $\sum_{i=1}^q ||o_i - \text{sim}(\mathbf{x}_i^{cf}, \mathbf{x}'_i)||_2^2$.

Thus the proposed algorithm has two phases:

Here is an example of how the method can be used to enforce positive individual treatment effects (ITE) among features. Consider an example of feature v and its causes (v_1, \dots, v_p) , with a positive ITE of each cause on the feature v . This can be captured implicitly by a simple Oracle O.

$$O(\mathbf{x}, \mathbf{x}^{cf}) = \begin{cases} 1, & \text{if } (\forall i \{ \mathbf{x}_{v_{pi}}^{cf} > \mathbf{x}_{v_{pi}} \} \implies \mathbf{x}_v^{cf} > \mathbf{x}_v) \text{ or} \\ & (\forall i \{ \mathbf{x}_{v_{pi}}^{cf} < \mathbf{x}_{v_{pi}} \} \implies \mathbf{x}_v^{cf} < \mathbf{x}_v) \\ 0, & \text{otherwise} \end{cases}$$

Additionally, the method can be used to capture personalized user-specific constraints with a user as the oracle, thus representing human perception. Different users could be modeled using different oracles. The oracle can give labelled data for (multiple) user-specific constraints by simply stating a counterfactual as feasible ($O(\mathbf{x}, \mathbf{x}') = 1$) or infeasible ($O(\mathbf{x}, \mathbf{x}') = 0$).

4 Empirical Evaluation

We evaluate our proposed methods, Model-based CF, Model-approx CF, and Example-Based CF on the Adult dataset and simulated Bayesian network datasets. For a fair comparison to Example-Based CF, we use its base bariational autoencoder as the base CF generator for both Model-based CF and Model-approx CF. As we have mentioned before, a counterfactual could be infeasible due to many reasons, but for our evaluation, we assume that there is a constraint that completely captures the feasibility of a counterfactual. To design this constraint, we either infer it from the causal model (simulated datasets) or from domain knowledge (real-world dataset).

4.1 Datasets.

Simple-BN. We consider a toy dataset of 10,000 samples with three features (x_1, x_2, x_3) and one outcome variable (y) . The causal relationships between them are modeled as:

$$\begin{aligned} p(x_1) &\sim N(\mu_1, \sigma_1); & p(x_2) &\sim N(\mu_2, \sigma_2) \\ p(x_3|x_1, x_2) &\sim N(k_1 * (x_1 + x_2)^2 + b_1, \sigma_3); k_1 > 0, b_1 > 0; \\ p(y|x_1, x_2, x_3) &\sim \text{Bernoulli}(\sigma(k_2 * (x_1 * x_2) + b_2 - x_3)); k_2 > 0, b_2 > 0 \end{aligned}$$

Note that we require x_1 and x_2 to be positive, so they follow a truncated normal distribution. The intuition is that x_3 is determined by a monotonically increasing function of x_1 and x_2 . At the same time, y is positively affected by an increase in x_1 and x_2 but negatively affected by x_3 . Thus, a naive

counterfactual method may not satisfy the monotonic constraint on $(\mathbf{x}_1, \mathbf{x}_2)$ and \mathbf{x}_3 . Specifically, the global monotonicity constraint is defined as: “ $(\mathbf{x}_1, \mathbf{x}_2$ increase $\implies \mathbf{x}_3$ increases) AND $(\mathbf{x}_1, \mathbf{x}_2$ decrease $\implies \mathbf{x}_3$ decrease)”).

We report results for a hand-crafted set of parameters such that it is possible to have a tradeoff between proximity and monotonic feasibility constraint: $\mu_1 = 50, \mu_2 = 50, \sigma_1 = 15, \sigma_2 = 17, \sigma_3 = 0.5, k_1 = 0.0003, k_2 = 0.0013, b_1 = 10, b_2 = 10$.

Sangiovese [11]. This is a conditional linear Bayesian network on the effects of different agronomic settings on quality of Sangiovese grapes [12]. It has 14 features and a categorical output for quality, with a sample size of 10,000. The true causal model is known. The features are all continuous except Treatment which has 16 levels. For simplicity, we remove the categorical variable Treatment since it leads to 16 different linear functions. For feasibility, we test a monotonic constraint over two variables, *BunchN* and *SproutN*. Specifically, the global monotonicity constraint is defined as:

$$(\text{SproutN increase} \implies \text{BunchN increases}) \text{ AND } (\text{SproutN decrease} \implies \text{BunchN decrease})$$

Adult [13]. We consider a real-world dataset, Adult. The outcome y is binary $y = 0$ (Low Income), and $y = 1$ (High Income). Since we do not have a causal model, we design two constraints that capture feasibility using domain knowledge:

$$\text{C1: } \mathbf{x}_{Age}^{cf} \geq \mathbf{x}_{Age}$$

$$\text{C2: } (\mathbf{x}_{Ed}^{cf} > \mathbf{x}_{Ed} \implies \mathbf{x}_{Age}^{cf} > \mathbf{x}_{Age}) \text{ AND } (\mathbf{x}_{Ed}^{cf} = \mathbf{x}_{Ed} \implies \mathbf{x}_{Age}^{cf} \geq \mathbf{x}_{Age})$$

C1 represents a unary constraint that Age cannot decrease in CF explanations. C2 represents a monotonic constraint that increase in Educational level should increase Age, and if Educational level remains the same, age should not decrease. C2 also includes an additional constraint that Education level cannot decrease. Hence, if Education level decreases then its an infeasible counterfactual, regardless of the change in Age (since in practice Education level does not usually decrease). To make the CF generation task more challenging, we sample data points with the Age feature greater than 35 and outcome class $y = 0$ and data points with the value of feature Age less than 45 and the outcome class $y = 1$. This creates a setup in which higher age data points are more correlated with the low income class group and vice-versa. We obtain a dataset of size 15691 and consider the task of generating CFs with the target class as $y = 1$.

4.2 Evaluation Setup

For all experiments, the ML classifier h is implemented as a neural network with two hidden layers, with non-linear activation (ReLU) on the first hidden layer. Continuous features are scaled to (0-1) range and categorical features are represented as one-hot encoded vectors. Each proposed method for counterfactual generation is trained using a 80-10-10% training, validation and test dataset respectively. For the Example-Based CF method, we additionally generate the query set Q using 10% of the training dataset with 10 counterfactuals per data point. Details regarding the ML model, the base VAE architecture, and hyperparameter tuning for all methods are provided in Suppl. C.1.

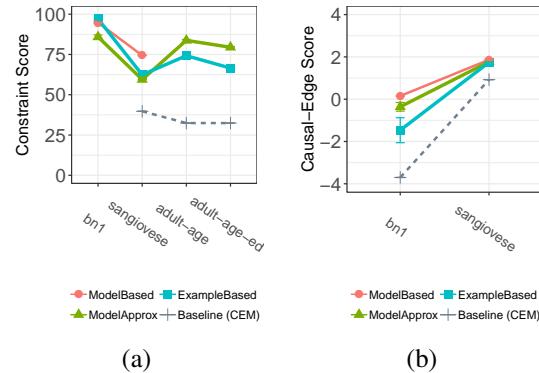


Figure 2: Constraint-Feasibility for three datasets, Causal-Edge score for BN1 and Sangiovese.

Methods. We compare results for Model-based CF, Model-approx CF, and Example-Based CF with CEM, the state-of-the-art contrastive explanations method proposed by [5] that uses an

auto-encoder to model probability distribution of train data. Suppl. C.1 describes the loss terms used for modeling constraints in Model-approx CF for different datasets.

Evaluation Metrics. We define the following metrics to evaluate CF examples.

- **Target-Class Validity:** % of CFs whose predicted class is the target class;
- **Cont-Proximity:** Proximity for continuous features as the average ℓ_1 -distance between x^{cf} and x in units of median absolute deviation for each features [7];
- **Cat-Proximity:** Proximity for categorical features as the total number of mismatches on categorical value between x^{cf} and x for each feature [7];
- **Constraint Feasibility Score:** For Simple-BN and Sangiovese datasets, the harmonic mean of % of CFs satisfying the two sub constraints (S1 and S2) of the given monotonic constraint, $\frac{2*S1*S2}{S1+S2}$, and for Adult we report % of CFs satisfying C1 and C2 separately;
- **Causal-Edge Score:** Log Likelihood of CFs w.r.t. a given causal edge distribution. Causal-Edge-Score is defined only for SimpleBN and Sangiovese where the true causal model is known.

We also evaluate on the Interpretability Score proposed in [14]; details are in Suppl. C.1.

4.3 Results

Evaluating feasibility. Figure 2 shows Constraint-Feasibility Score for all datasets and Causal Edge Score for Simple-BN and Sangiovese datasets, averaged over 10 runs (other metrics are in the Suppl. C.2). For Simple-BN dataset, Example-Based CF achieves the highest Constraint Feasibility score, Model-based CF achieve the highest Constraint Feasibility score on the Sangiovese dataset, while the Model-approx CF achieves the highest Constraint Feasibility score on the Adult dataset.

All the methods achieve perfect score on the Target-Class Validity (refer to Suppl. C.2). However, across the three datasets, the methods designed to preserve feasibility (Model-based CF, Model-approx CF, and Example-Based CF) perform better than CEM on the Constraint-Feasibility Score. That is, CEM achieves a score of zero on simple-bn dataset and around 40% on the Sangiovese and Adult dataset.

The poor performance of CEM on Constraint Feasibility across datasets suggests that feasibility cannot be solely captured by relying on the observed data likelihood. In the Adult dataset, the feasibility constraint requires Age to be increased, despite a correlation between low Age and High Income in the dataset, illustrating the fact that following observed distribution does not ensure feasibility.

We also compare on the Causal-Edge score metric that evaluates the log-likelihood of the generated CF wrt the true function in the causal graph. For Simple-BN dataset, we find that Model-Based method achieves the highest score, followed by Model-Approx and Example-Based. On Sangiovese, all methods are comparable. While the Model-Based and Model-Approx methods have explicit knowledge of the constraints, this result shows that the Example-Based method can also learn the constraint based on examples. CEM method has the lowest score.

Example-Based CF: Constraint Feasibility increases with no. of labelled CFs. A key question for the Example-Based method is the number of labelled CF examples it needs. Using the Adult dataset and the non-decreasing Age constraint, we show the Constraint-Feasibility Score of Example-Based CF as we increase the number of labelled CF examples (Figure 3 (a)). For the global constraint, we find that the Feasibility Score increases with labelled inputs, reaching nearly 80% with 100 labels. Compared to prior work that does a separate optimization for each CF [5, 7], Example-Based method is also computationally efficient. We show its comparison to CEM in

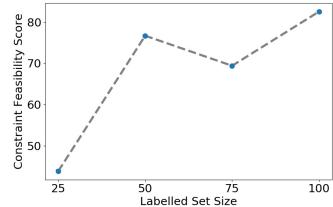


Figure 3: Constraint-Feasibility score as the no. of labelled examples is increased for global constraints in Adult.

Suppl.D.

BaseVAE for CF generation Apart from feasibility, we conduct experiments with the BaseVAE method to test it for CF example generation on MNIST; the details can be found in the section Suppl. E.

5 Related Work

Our work builds upon the literature on explainable ML [1, 15] by focusing on a specific type of explanation through counterfactual examples [2]. Most CF generation methods rely on separate optimizations for each input, based on original features [16, 7], a latent representation [17], or using a generative adversarial network [18]. We also build on the fundamental work on counterfactuals [8].

To account for feasibility, different statistical notions of feasibility have been proposed, based on adherence to the training distribution [5], distribution of the target class [14], the likelihood of the intermediate points in reaching a CF example [6], and on specifying which features can be changed [4]. [18] rely on GAN’s to restrict the explanations in semantically meaningful space. In a critical commentary, [19] raise concern that feasibility cannot be learned only from training data distribution. Related to our framework on expressing feasibility in terms of causal constraints, [7] point to the importance of causal constraints for feasibility, but do not provide a method for generating feasible CF examples. Our paper extends this line of work by formally defining feasibility, providing a theoretical justification of the counterfactual loss and proposing a VAE-based generative model that can preserve causal constraints. [20, 21, 17] also focus on the role of causality towards feasible counterfactual explanations but their approach requires full knowledge of the causal model.

6 Conclusion

Feasibility in CF explanations is hard to quantify. In this work, we provided a generative model and two methods for modeling causal constraints. In future work, we will explore how to integrate domain knowledge and available data to learn causal constraints.

References

- [1] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. Why should i trust you?: Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, pages 1135–1144. ACM, 2016.
- [2] Sandra Wachter, Brent Mittelstadt, and Chris Russell. Counterfactual explanations without opening the black box: Automated decisions and the gdpr. *Harv. JL & Tech.*, 31:841, 2017.
- [3] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014.
- [4] Berk Ustun, Alexander Spangher, and Yang Liu. Actionable recourse in linear classification. In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, pages 10–19, 2019.
- [5] Amit Dhurandhar, Pin-Yu Chen, Ronny Luss, Chun-Chen Tu, Paishun Ting, Karthikeyan Shanmugam, and Payel Das. Explanations based on the missing: Towards contrastive explanations with pertinent negatives. In *Advances in Neural Information Processing Systems*, pages 592–603, 2018.
- [6] Rafael Poyiadzi, Kacper Sokol, Raul Santos-Rodriguez, Tijl De Bie, and Peter Flach. Face: Feasible and actionable counterfactual explanations. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pages 344–350, 2020.
- [7] Ramaravind Kommiya Mothilal, Amit Sharma, and Chenhao Tan. Explaining machine learning classifiers through diverse counterfactual explanations. In *Proceedings of the ACM FAT* conference (to appear)*, 2020.
- [8] Judea Pearl. *Causality*. Cambridge University Press, 2009.
- [9] Diederik P Kingma and Max Welling. Auto-encoding variational bayes. *arXiv preprint arXiv:1312.6114*, 2013.
- [10] Kihyuk Sohn, Honglak Lee, and Xinchen Yan. Learning structured output representation using deep conditional generative models. In *Advances in neural information processing systems*, pages 3483–3491, 2015.

- [11] Alessandro Magrini, Stefano Di Blasi, and Federico Mattia Stefanini. A conditional linear gaussian network to assess the impact of several agronomic settings on the quality of tuscan sangiovese grapes. *Biometrical Letters*, 2017.
- [12] Bayesian network repository. <http://www.bnlearn.com/bnrepository/> sangiovese.
- [13] Ronny Kohavi and Barry Becker. Uci machine learning repository. <https://archive.ics.uci.edu/ml/datasets/adult>, 1996.
- [14] Arnaud Van Looveren and Janis Klaise. Interpretable counterfactual explanations guided by prototypes. *arXiv preprint arXiv:1907.02584*, 2019.
- [15] Scott M Lundberg and Su-In Lee. A unified approach to interpreting model predictions. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, *Advances in Neural Information Processing Systems 30*, pages 4765–4774. Curran Associates, Inc., 2017.
- [16] Chris Russell. Efficient search for diverse coherent explanations. In *Proceedings of FAT**, 2019.
- [17] Shalmali Joshi, Oluwasanmi Koyejo, Warut Vigitbenjaronk, Been Kim, and Joydeep Ghosh. Towards realistic individual recourse and actionable explanations in black-box decision making systems. *arXiv preprint arXiv:1907.09615*, 2019.
- [18] Shusen Liu, Bhavya Kailkhura, Donald Loveland, and Yong Han. Generative counterfactual introspection for explainable deep learning. *arXiv preprint arXiv:1907.03077*, 2019.
- [19] Solon Barocas, Andrew D Selbst, and Manish Raghavan. The hidden assumptions behind counterfactual explanations and principal reasons. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, pages 80–89, 2020.
- [20] Álvaro Parafita and Jordi Vitrià. Explaining visual models by causal attribution. *arXiv preprint arXiv:1909.08891*, 2019.
- [21] Amir-Hossein Karimi, Bernhard Schölkopf, and Isabel Valera. Algorithmic recourse: from counterfactual explanations to interventions. *arXiv preprint arXiv:2002.06278*, 2020.
- [22] Algorithms for monitoring and explaining machine learning models. <https://docs.seldon.io/projects/alibi> alibi.
- [23] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.

A Supplementary Materials: Theorem 1 Proof

Theorem 2. *The evidence lower bound to optimize CF objective $\Pr(\mathbf{x}^{cf}|y', \mathbf{x})$ for global feasibility is:*

$$\begin{aligned} \ln \Pr(\mathbf{x}^{cf}|y', \mathbf{x}) &\geq \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x}) \\ &\quad - \mathbb{KL}(Q(\mathbf{z}|\mathbf{x}, y')||P(\mathbf{z}|y', \mathbf{x})) \end{aligned} \quad (2)$$

Proof. An ideal counterfactual generation model approximates \mathbf{x} (proximity) and generates \mathbf{x}^{cf} that are valid w.r.t desired class y' . Thus for a model we seek to maximize $P(\mathbf{x}^{cf}|y', \mathbf{x})$ where P is the underlying probability distribution over \mathcal{X} .

$$\begin{aligned} &\ln P(\mathbf{x}^{cf}|y', \mathbf{x}) \\ &= \ln \int P(\mathbf{x}^{cf}, \mathbf{z}|y', \mathbf{x}) d\mathbf{z} \\ &= \ln \int Q(\mathbf{z}|\mathbf{x}, y') \frac{P(\mathbf{x}^{cf}, \mathbf{z}|y', \mathbf{x})}{Q(\mathbf{z}|\mathbf{x}, y')} d\mathbf{z} \\ &\geq \int Q(\mathbf{z}|\mathbf{x}, y') \ln \frac{P(\mathbf{x}^{cf}, \mathbf{z}|y', \mathbf{x})}{Q(\mathbf{z}|\mathbf{x}, y')} d\mathbf{z} \\ &= \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln \frac{P(\mathbf{x}^{cf}, \mathbf{z}|y', \mathbf{x})}{Q(\mathbf{z}|\mathbf{x}, y')} \\ &= \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x}) - \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln \frac{Q(\mathbf{z}|\mathbf{x}, y')}{P(\mathbf{z}|y', \mathbf{x})} \end{aligned} \quad (3)$$

Where the inequality above is due to Jensen's inequality. Using the definition of KL-Divergence,

$$\begin{aligned} \ln P(\mathbf{x}^{cf}|y', \mathbf{x}) &\geq \mathbb{E}_{Q(\mathbf{z}|\mathbf{x}, y')} \ln P(\mathbf{x}^{cf}|\mathbf{z}, y', \mathbf{x}) \\ &\quad - \mathbb{KL}(Q(\mathbf{z}|\mathbf{x}, y')||P(\mathbf{z}|y', \mathbf{x})) \end{aligned}$$

□

B Defining CF explanations as Interventions on a Structural Causal Model

In Section 2 we provided a novel distance metric that captures the feasibility of perturbations from the original input, based on a structural causal model (SCM) that describes causal relationships between different features. Since changing a feature x_v can change the values of other features, the SCM helps us model the downstream changes due to change in x_v . However, unlike the standard SCM intervention that cuts off all incoming edges (causes) on the perturbed features [21], we assume that the perturbed feature can also be affected by its other causes. This is because CF explanations are intended to present perturbations that are feasible in the real world and it is unlikely for a person to change a feature to any value independent of its causes. That is, any suggested perturbation in a feature that does not satisfy its relationship with its causal parents will not be possible in the real world.

For example, consider the features represented by the SCM in Figure 4 where we assume that an ML model uses these features to predict a loan decision. Perturbing house rent can be considered as an intervention that affects savings of a person and may also lead to a counterfactual example by changing their original decision outcome. However house rent cannot be changed independently of the person's income (its causal parent in Figure 4): a simple feasibility constraint is that (perturbed) house rent cannot exceed (optionally perturbed) income in any CF example. Therefore, rather than independent interventions that are suitable when estimating causal effect (e.g., estimating the effect of a drug treatment through a randomized experiment), we employ a modified version where the causes continue to affect the perturbed feature.

In situations where an independent intervention on features is possible, those features can be considered as exogenous variables U when computing the DistCausal metric from Section 2.3 (under a modified SCM wherein incoming edges to such features are cut off).

Comparison to the standard proximity metric for CF explanations. Note that unlike the standard distance metric for proximity, we do not compare the proposed x_v^{cf} to the original input's feature value x_v , but rather

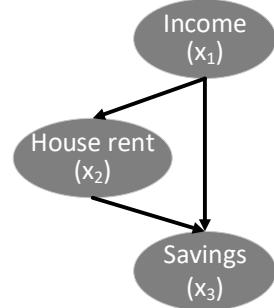


Figure 4: SCM describing the true causal relationships between three input features: Income, House rent, and Savings of a person. These input features are used by a pre-trained black-box ML model that we wish to explain.

compare x_v^{cf} to its predicted value $f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf})$ based on the values of its causal parents in \mathbf{x}^{cf} . Here $f : \mathbb{E}[x_v | x_{vp1}, \dots, x_{vpk}]$ is the conditional expected value based on the SCM.

When the distance metric is ℓ_2 , the above can be equivalently written as the distance between the *relative* change between x_v and x_v^{cf} , and the expected change between $f(x_{v_{p1}}, \dots, x_{v_{pk}})$ and $f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf})$ as predicted by the SCM.

$$\begin{aligned}\Delta_v &= x_v^{cf} - x_v \\ \Delta_{predictedv} &= (f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}) + \epsilon_1) - (f(x_{v_{p1}}, \dots, x_{v_{pk}}) + \epsilon_2) \\ \mathbb{E}[\Delta_{predictedv}] &= f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}) - f(x_{v_{p1}}, \dots, x_{v_{pk}})\end{aligned}\tag{4}$$

where ϵ_1 and ϵ_2 are mutually independent zero-mean errors. Then the distance can be written as,

$$\begin{aligned}\text{DistCausal}_v(x_v, x_v^{cf}) &= \text{Dist}(\mathbb{E}[\Delta_v], \mathbb{E}[\Delta_{predictedv}]) \\ &= \ell_2(x_v^{cf}, f(x_{v_{p1}}^{cf}, \dots, x_{v_{pk}}^{cf}))\end{aligned}\tag{5}$$

averaged over different input values.

C Implementation Details and Results on Bayesian Networks and Adult Dataset

Here we provide implementation details and additional results on the Bayesian network and Adult datasets.

C.1 Implementation Details

C.1.1 ML Model Architecture

We first describe the architecture of the ML model. The ML model for all the datasets was trained for 100 epochs, batch size 32, learning rate 10^{-3} with Adam optimizer and Cross Entropy Loss, with 80-10-10% training, validation and test datasets. It achieved test accuracy of 87% on Simple-BN, 83.5% on Sangiovese, and 89.3% on Adult dataset.

Each ML model comprises of two layers as shown below:

- Hidden Layer(data-size, hidden-dim)
- Hidden Layer(hidden-dim, num-classes)

The values of *hidden-dim* is chosen as 10 and value of *num-classes* is 2 as it is a binary classification task across the three datasets.

C.1.2 BaseVAE Architecture

Here we provide the implementation details of the base variational encoder decoder used in all our different methods. Both the encoder and decoder are modeled as Neural Networks (NN) with multiple hidden layers and non linear activations. Encoder comprises of two Neural Networks: one NN is used to estimate the mean and other NN is used to estimate the variance of posterior distribution $q(z|x, y_k)$. Both the networks for estimating mean and variance have the same architecture as described below, with the only difference that the variance network having an additional Sigmoid activation at the end to ensure the variance is positive. Similarly, decoder comprises of a neural network to estimate the counterfactual from the latent encoding and the target class.

Encoder Architecture:

- Hidden Layer 1(DataSize+1, 20), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 2(20, 16), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 3(16, 14), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 4(14, 12), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 5(12, LatentDim)
- Sigmoid (In case of variance network only)

Decoder Architecture:

- Hidden Layer 1(LatentDim+1, 12), BatchNorm, Dropout(0.1), ReLU

- Hidden Layer 2(12, 14), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 3(14, 16), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 4(16, 20), BatchNorm, Dropout(0.1), ReLU
- Hidden Layer 5(20, DataSize), Sigmoid

The latent space dimension (*LatentDim*) is set to 10 for all the different methods and datasets. Both the encoder and the decoder are conditioned on the target counterfactual class. Hence, the **Hidden Layer 1** in the Encoder takes the data point concatenated with the target class as the input. Similarly, the **Hidden Layer 1** in the Decoder takes the latent sample concatenated with the target class as the input.

For all datasets, we use the SGD optimizer with learning rate 10^{-3} for 50 epochs. The batch size for the different datasets are: Simple-BN : 64, Sangiovese : 512, Adult : 2048.

C.1.3 Contrastive Explanations

For experiments involving the Contrastive Explanations (CEM) method [5], we used the implementation provided by the open source library ALIBI [22]. Since the choice of auto encoder is not specified in ALIBI, we use an auto encoder with the same architecture as defined above in *Base VAE Architecture* section for a fair comparison. The only difference being that the Encoder and Decoder are not conditioned on the target class.

C.1.4 HyperParameter tuning

For a fair comparison between methods, we optimize hyperparameters using the validation set and use random search for 100 iterations. Since an ideal counterfactual needs to satisfy feasibility, target-class validity, and proximity, we select the hyperparameters that lead to maximum feasibility, while still obtaining more than 90% target class validity and proximity at least τ . τ was conservatively selected to remove models that result in much lower proximity than the BaseVAE method (and thus will be less useful in practice). In our experiments, we found that all methods achieved near 100% target-class validity.

The following threshold values of τ were used depending on the dataset:

- BN1: 9.0 (Cont. Proximity)
- Sangiovese: 20.0 (Cont. Proximity)
- Adult: 8.0 (Cont. Proximity) and 5.0 (Cat. Proximity)

We did not include the other metrics like Interpretability Score and Causal Edge score during the hyperparameter tuning, to allow an independent evaluation on those metrics.

The final optimal values of the hyper parameters for each dataset are reported in Table 1. As per the *BaseGenCFLoss* equation (section 3.1), we have the two hyperparameters β and λ common across all the approaches; which we refer to as **Margin** and **Validity** in the table 1.

Additionally, there is an extra hyperparameter involved with approaches like **Model-based CF**, **Model-approx CF**, and **Example-Based CF**. We denote this extra hyperparameter as **Feasibility** in the Table 1. For **Example-Based CF**, it corresponds to λ_o which controls the trade-off between modeling CF and the oracle (Section 3.2). In the case of **Model-based CF**, it corresponds to the trade-off between Exogenous and Endogenous Loss terms in *DistCausal* loss term, as described below:

$$\text{DistCausal}(\mathbf{x}, \mathbf{x}^{cf}) = \sum_{u \in U} \text{Dist}_u(\mathbf{x}_u^{cf}, \mathbf{x}_u) + \lambda_s * \sum_{v \in V} \text{DistCausal}_v(\mathbf{x}_v, \mathbf{x}_v^{cf})$$

In the case of **Model-approx CF**, for Unary constraints, it corresponds to the trade-off between *BaseGenCFLoss* and the Hinge Loss on feature of interest. For the Binary constraints, it would follow the same procedure as for **Model-based CF**.

For the Contrastive Explanations (CEM) method, the optimal hyperparameters for each dataset are as follows: (refer to open source library ALIBI [22] for details regarding each hyper parameter)

- Simple BN: Beta (0.608), Kappa (0.021), Gamma (8.0), CSteps (3), Max Iterations (1000)
- Sangiovese: Beta (0.652), Kappa (0.041), Gamma (9.0), CSteps (5), Max Iterations (1000)
- Adult: Beta (0.911), Kappa (0.241), Gamma (0.0), CSteps (9), Max Iterations (1000)

Table 1: Hyperparameter tuning description for all the methods and datasets

Dataset	Method	Margin	Validity	Feasibility
Simple-BN	Model-approx CF	0.087	96	0.1
	Example-Based CF	0.15	150	2350
	Model-based CF	0.015	85	55
Sangiovese	Model-approx CF	0.306	71	73
	Example-Based CF	0.02	25	1085
	Model-based CF	0.319	89	77
Adult-Age	Model-approx CF	0.764	29	192
	Example-Based CF	0.084	159	5999
Adult-Age-Ed	Model-approx CF	0.344	76	87
	Example-Based CF	0.117	175	3807

C.1.5 Evaluation Metrics

We define the following metrics to evaluate CF explanations; considering the case of N data points $\{x_i\}$, with K CF's $\{x_{i,j}^{cf}\}$ sampled for each data point.

- **Target-Class Validity:** % of CFs whose predicted class by the ML classifier is the same as the target class: $\frac{\sum_{i=1}^N \sum_{j=1}^K \mathbb{1}[f(x_{i,j}^{cf}) == t_c]}{N*K}$.
- **Cont-Proximity:** Proximity for continuous features as the average ℓ_1 -distance between x^{cf} and x in units of median absolute deviation for each features [7]; It is multiplied by (-1) so that higher values are better.

$$\frac{\sum_{i=1}^N \sum_{j=1}^K \sum_{p=1}^{d_{cont}} \frac{x_{i,j}^{cf,p} - x_i^p}{MAD_p}}{N*K*d_{cont}}$$
- **Cat-Proximity:** Proximity for categorical features as the total number of mismatches on categorical value between x^{cf} and x for each feature [7]; It is multiplied by (-1) so that higher values are better.

$$\frac{\sum_{i=1}^N \sum_{j=1}^K \sum_{p=1}^{d_{cat}} \mathbb{1}[x_{i,j}^{cf,p} \neq x_i^p]}{N*K*d_{cat}}$$
- **Constraint Feasibility Score:** For Simple-BN and Sangiovese datasets, the constraints mentioned can be observed as a combination of two sub constraints: X1 and X2. For example, in the case of Simple-BN dataset, X1 corresponds to “(x_1, x_2 increase $\implies x_3$ increases)”; while X2 correspond to “(x_1, x_2 decrease $\implies x_3$ decrease)”

Hence, to ensure good performance at satisfying both sub-constraints, we define the following metric for constraint feasibility: $\frac{2*S1*S2}{S1+S2}$ where S1, S2 represent the % of CFs satisfying the sub constraints X1, X2 respectively.

However in the case of Adult dataset, due to the additional non monotonic constraint of Education level cannot decrease, we simply report the percentage of Counterfactual satisfying the complete constraint C2 on the Adult dataset.

For unary constraints, like C1 on the Adult dataset, we always report the percentage of Counterfactuals satisfying the constraint.

- **Causal-Edge Score:** Ratio of the Log Likelihood of CFs x^{cf} and the Log Likelihood of the original data point x w.r.t. to the set of given causal edges distribution V : $\frac{\sum_{i=1}^N \sum_{j=1}^K \sum_{v \in V} \frac{\log p(x_{v,1}^{cf} | x_{v,2}^{cf}, \dots, x_{v,K}^{cf})}{\log p(x_v | x_{v,1}, \dots, x_{v,K})}}{N*K}$
- **Interpretability Score:** The IM1 metric as defined by [14], the ratio of the reconstruction loss of CFs given the target class Auto Encoder and the reconstruction loss given the original class Auto Encoder :

$$\frac{\sum_{i=1}^N \sum_{j=1}^K \frac{\|x^{cf} - AE_t(x^{cf})\|}{\|x^{cf} - AE_o(x^{cf})\|}}{N*K}$$
. Thus, lower IM1 score is better.

C.1.6 Constraint Modelling in Model-approx CF

For the case of Simple-BN and Sangiovese dataset, the feasibility constraint is monotonic, hence we use the *Binary Constraints* formulation of Model-approx CF, as described in the Section 2.4 in the main submission.

For the case of Adult Dataset, the constraint C1 is modelled using the *Unary Constraints* formulation, with a Hinge Loss on the feature Age. The constraint C2 in Adult Dataset is more complex than the previous constraints, since the feature Education is categorical. We model the constraint C2 under the *Unary Constraints* formulation, since it can be viewed as combinations of two unary constraints: Age cannot decrease and Education cannot decrease. The Hinge Loss on categorical variable Education is implemented by converting the embedding of categorical variable Education into a continuous value. We rank different education levels with increasing score

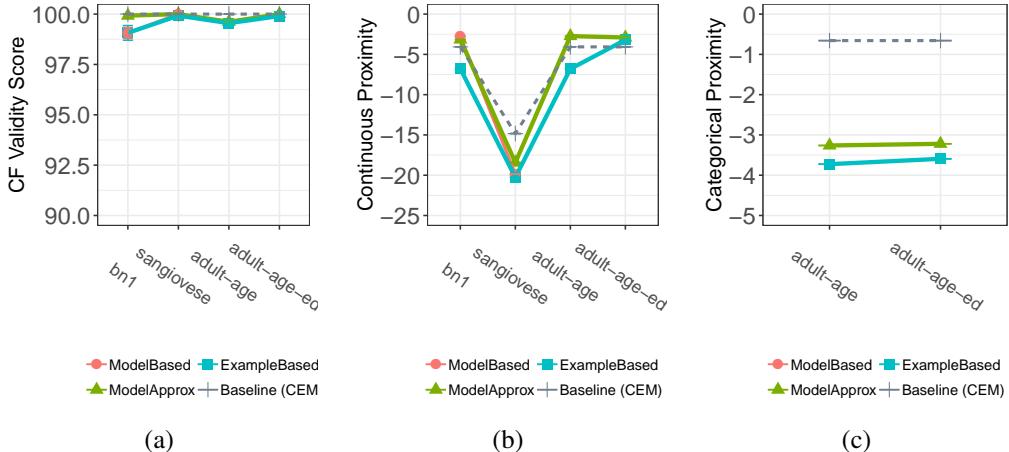


Figure 5: Validity, Continuous Proximity and Categorical Proximity metrics for different CF explanation methods.

and take a weighted sum of the categorical embedding with the scores assigned for each education category. Hence, we get a continuous score for education feature embedding which is representative of the level/rank of education. Now, we can apply the same Hinge Loss on the continuous values of education feature to put penalty on counterfactuals that decrease the level of education.

The vector we used for ranking different educations levels is as follows:

- HS-Grad, School: 0
- Bachelors, Assoc, Some-college: 1
- Masters:2
- Prof-school, Doctorate: 3

C.2 Evaluation Results on Additional Metrics

Target-Class Validity: Figure 5(a) shows the performance of the methods on Target-Class Validity. All the methods achieve near perfect score on this metric across datasets.

Continuous Proximity: Figure 5(b) shows the methods evaluated on the Cont-Proximity metric. The dataset Sangiovese shows an interesting trend where the approaches with higher Constraint-Feasibility score (Model-based CF, Model-approx CF, Example-Based CF) perform worse on Cont-Proximity metric as compared to the approaches with lower Constraint-Feasibility score (Baseline (CEM)). This suggests increasing feasibility might induce a trade-off with the continuous proximity in some cases.

Categorical Proximity: Figure 5(c) shows the methods evaluated on the Cat-Proximity metric. The dataset Simple-BN and Sangiovese do not contain any categorical variables, hence we do not include them for this analysis. CEM performs better than other methods on Categorical proximity in both the cases of age (C1) and age-ed (C2) constraint. This may be because CEM tends to not vary categorical features. Table 2 provides an example via generated CF examples for the Adult dataset: CEM does not change categorical features like Occupation, MaritalStat, Race unlike Model-approx CF and Example-Based CF. Along with Figure 5(b), this result demonstrates the trade-off between feasibility and proximity. CEM is worse at preserving constraints (e.g., in Table 2, CF examples by CEM do not increase the value of Age while increasing the Education level to Masters), but achieves higher proximity score for categorical variables.

Interpretability Score: Figure 6 shows the performance of the methods on the Interpretability score (IM1 metric). Model-based CF and Model-approx CF consistently perform better than Baseline (CEM) across different datasets, which suggests that Model-based CF and Model-approx CF do not generate counterfactuals that are far away from the data distribution while preserving feasibility constraints. Also, Example-Based CF performs worse than Baseline (CEM) on the adult-age dataset despite obtaining a higher Constraint-Feasibility score (Figure 2(a)). This suggests that generating counterfactuals closer to the data distribution is not guaranteed to provide feasibility.

Table 2: Examples of generated counterfactuals on the modified Adult dataset. Example-Based CF and Model-approx CF were trained to preserve the Education-Age causal constraint

Adult	Method	AgeYrs	Education	Occupation	WorkClass	Race	HrsWk	MaritalStat	Sex
Original input (outcome: <=50K)		41	Some-college	Blue-collar	Private	Other	40	Single	Male
Counterfactuals (outcome: >50K)	Model-approx CF	46	Masters	White-Collar	Private	White	41	Married	Male
		45	Some-college	White-Collar	Private	White	40	Married	Male
		47	Masters	White-Collar	Private	White	41	Married	Male
Counterfactuals (outcome: >50K)	Example-Based CF	45	Prof-school	White-Collar	Private	White	42	Married	Male
		44	Masters	White-Collar	Private	White	42	Married	Male
		47	Prof-school	White-Collar	Private	White	43	Married	Male
Counterfactuals (outcome: >50K)	Baseline (CEM)	41	Masters	Blue-Collar	Private	Other	39	Single	Male
		41	Some-college	Blue-Collar	Other	Other	39	Single	Male
		40	Masters	Blue-Collar	Private	Other	41	Single	Male

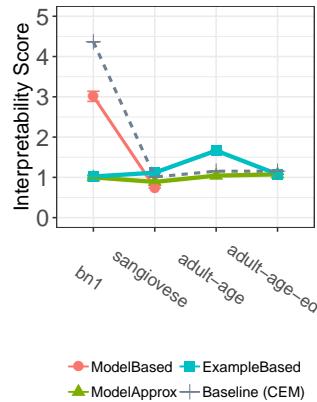


Figure 6: Interpretability score (IM1) for different CF generation methods. Lower IM1 score is better.

D Computational Efficiency of Example-Based CF

Besides feasibility, Example-Based CF is computationally faster than past methods like CEM, since it uses a generative model. In Figure 8, we show the time required to generate counterfactual examples for k inputs for the Adult dataset and find that Example-Based CF takes less time per CF example as k increases. CEM has a non-trivial execution time for each input while Example-Based CF takes time for initial training but then negligible time for every new input. Since Model-based CF and Model-approx CF also rely on a VAE architecture, they are similarly efficient to Example-Based CF.

Additional metrics for Figure 3(a). In Figure 3, we showed the Constraint-Feasibility score as the number of labelled examples from the Adult dataset are increased for the Example-Based CF method. Here we show additional metrics in Figure 7: Target-Class Validity, Continuous Proximity and Categorical Proximity. While we saw a substantial increase in the Constraint-Feasibility Metric (Figure 3 in the main submission), we find that other metrics on validity and proximity do not change much, as the number of labelled examples increases from 25 to 100.

E Supplementary Materials: Applying Base VAE to an Image Dataset

Finally, to show the generality of the proposed method, we apply the BaseVAE CF generator on the MNIST dataset [23] which contains 70,000 labeled 28x28 images of handwritten digits between 0 and 9. As the ML model to be explained, we train a neural network model on the dataset to predict the digit classes. For explaining this model, we consider the counterfactual generation task on 5 digits (2, 3, 4, 5, 8); with the respective target counterfactual classes (3, 5, 9, 3, 9) as shown in Figure 9. We take a subset of 100 samples for each of the 5 digits for training the BaseVAE method. Details on the model architecture for the ML model and BaseVAE are provided in section E.2

E.1 Results

Figure 9 shows the counterfactuals generated by our BaseVAE approach. Additionally, for evaluation we use two metrics defined by [14]: IM1 metric which measures the ratio between the reconstruction of x_{cf} using

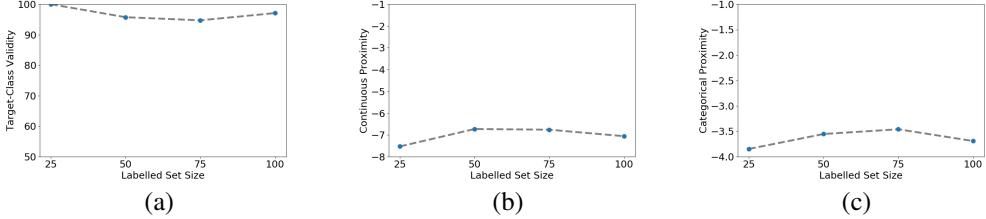


Figure 7: Target-Class Validity, Continuous Proximity and Categorical Proximity as Example-Based CF is trained on more labelled examples in the Adult dataset.

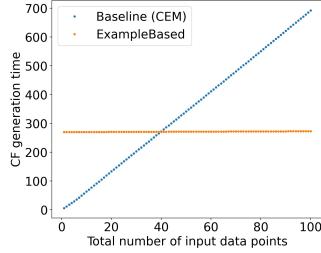


Figure 8: Comparison of the time taken to generate CF examples for the proposed Example-Based CF method and the baseline CEM method. After about 40 inputs, Example-Based CF is faster than CEM for generating CF examples.

AutoEncoders trained on target class and original class data: $IM1 = \frac{\|\mathbf{x}^{cf} - AE_t(\mathbf{x}^{cf})\|}{\|\mathbf{x}^{cf} - AE_o(\mathbf{x}^{cf})\|}$, and the IM2 metric, that measures the difference between the reconstruction of \mathbf{x}_{cf} using AutoEncoders trained on the target class and all classes: $IM2 = \frac{\|AE(\mathbf{x}^{cf}) - AE_t(\mathbf{x}^{cf})\|}{\|\mathbf{x}^{cf}\|}$.

To ensure a fair comparison; we used the same ML model and AutoEncoder architecture as [14] for computing the Interpretability Metrics (Table 3). The results reported for BaseVAE approach are the mean and standard deviation over 10 runs.

BaseVAE achieves a better IM1 and IM2 score than other approaches, even though it does not explicitly have an autoencoder term in its loss, unlike (B, C, D, E, F) approaches that use the AE or Prototype loss. These results are probably since our BaseVAE generative model, being trained on the full train data, is able to capture the feature distribution better.

That said, it is harder to interpret IM2 metric; Table 4 breaks down the performance of the BaseGenCF method on the IM1 and IM2 metric by analyzing the performance on its different components. IM1 Numerator corresponds to the reconstruction loss with the target class Auto Encoder: $\|\mathbf{x}^{cf} - AE_t(\mathbf{x}^{cf})\|$; while the IM1 Denominator corresponds to the reconstruction loss with the original class Auto Encoder: $\|\mathbf{x}^{cf} - AE_o(\mathbf{x}^{cf})\|$.

IM2 Numerator corresponds to the difference between the reconstruction loss using AutoEncoders trained on the target class and all classes: $\|AE(\mathbf{x}^{cf}) - AE_t(\mathbf{x}^{cf})\|$; while the IM2 Denominator corresponds to the norm of the counterfactual: $\|\mathbf{x}^{cf}\|$. Note that any method's performance on the IM2 metric would depend a lot on the norm of counterfactuals generated (IM2 Denominator), which may not be desirable. This limits a proper interpretation of the IM2 Metric as proposed by [14].



Figure 9: CF examples generated from MNIST images; the top row denotes the image and the bottom row denotes the associated counterfactual. In each case, a target class (*digit*) for the counterfactual was provided to the BaseVAE method.

To enable a better comparison, here we report the performance of our method BaseVAE on both components of IM2 metric. We do not have results of [14] on the different components of IM1 and IM2 metric, hence it is unclear why we obtain substantially better results on IM2 Metric (Table 3). It may be due to less reconstruction error difference (IM2 Numerator) or due to higher norm counterfactuals (IM2 Denominator) generated by our method.

Time Complexity: In addition, the time taken to generate CFs by BaseVAE is order of magnitude lower than other approaches. That said, we do have a fixed training time (**172.81 ± 3.97** seconds); thus our approach will be efficient for deployments where it can be trained once and used for generating multiple CFs for different inputs.

Table 3: Results for the MNIST dataset. Metrics for other approaches are from Table 1 in [14]

Method	Time (s)	Gradient Steps	IM1	IM2(*10)
A: V	13.06 ± 0.23	5158 ± 82	1.56 ± 0.03	1.65 ± 0.04
B: VA	8.40 ± 0.38	2380 ± 113	1.36 ± 0.02	1.60 ± 0.03
C: VP	2.37 ± 0.09	751 ± 31	1.23 ± 0.02	1.46 ± 0.03
D: VAP	2.05 ± 0.08	498 ± 27	1.26 ± 0.02	1.29 ± 0.03
E: P	4.39 ± 0.04	1794 ± 12	1.20 ± 0.02	1.52 ± 0.03
F: PA	2.86 ± 0.06	773 ± 16	1.22 ± 0.02	1.29 ± 0.03
BaseVAE	0.033 ± 0.001	600 (Training)	1.07 ± 0.07	0.12 ± 0.03

Table 4: Additional results for the MNIST dataset for the BaseVAE approach

Metric	Performance (mean ± std)
IM1 Numerator	3.37 ± 0.21
IM1 Denominator	3.32 ± 0.24
IM2 Numerator	1.02 ± 0.09
IM2 Denominator	107.04 ± 0.46

E.2 Implementation Details

The ML Model architecture and the BaseVAE architecture was kept the same as [14]. The details can be seen in this notebook by [14]. We describe the implementation details of the ML model and BaseVAE below.

E.2.1 ML Model Architecture

Architecture of the ML model to be explained is now described. A slight difference we had to introduce from the architecture of [14] was to make *kernel-size* as 3 (instead of 2) and *padding* as 1 to ensure the spatial dimensions of the image are the same as them after applying Conv Layer. The model was trained for 50 epochs, batch size 32, learning rate 10^{-4} with Adam optimizer and Cross Entropy Loss, with a 80-10-10% training, validation and test dataset respectively. It achieved test accuracy of 96%.

- Conv Layer(out-channels=32, kernel-size=3, stride=1, padding=1), ReLU
- MaxPool(pool-size=2), Dropout(0.3)
- Conv Layer(out-channels=64, kernel-size=3, stride=1, padding=1), ReLU
- MaxPool(pool-size=2), Dropout(0.3)
- Hidden Layer 1(256), Dropout(0.5), ReLU
- Hidden Layer 2(10), Softmax

E.2.2 Auto Encoder Architecture

The training strategy used was exactly the same as mentioned in the notebook by [14].

Architecture of the Encoder used for computing the IM1, IM2 Metrics:

- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- MaxPool(pool-size=2)
- Conv Layer(out-channel=1, kernel-size=3, stride=1, padding=0), ReLU

Architecture of the Decoder used for computing the IM1, IM2 Metrics:

- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- UpSample((2,2))
- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- Conv Layer(out-channel=1, kernel-size=3, stride=1, padding=0)

E.2.3 BaseGenCF Architecture

The BaseVAE Encoder Decoder framework as trained for 25 epochs, batch size 16, learning rate 10^{-4} with SGD optimizer and `BaseGenCFLoss` (Section 3.1), with a 80-10-10% training, validation and test dataset.

Encoder Architecture:

Architecture of Encoder consists of two networks: one is used to estimate the mean and the other is used to estimate the variance of the posterior distribution $q(z|x, y_k)$. Both the networks for estimating mean and variance have the same architecture as described below, with the only difference that the variance network having an additional Sigmoid activation at the end to ensure the variance is positive.

The network consists of sub models: the output from the sub model M1 is concatenated with the target class of the counterfactual and then fed into the sub model M2. We denote the size of the input after sub model M1 as *convoluted-size* and the latent embedding space dimension as *embedding-size*. We used *embedding-size* as 10 and the *convoluted-size* can be computed using the M1 architecture below to be $22 * 22$

Sub Model M1:

- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- Conv Layer(out-channel=16, kernel-size=3, stride=1, padding=0), ReLU
- Conv Layer(out-channel=1, kernel-size=3, stride=1, padding=0), ReLU

Sub Model M2:

- Hidden Layer(convoluted-size+1, embedding-size), BatchNorm
- Sigmoid (In case of variance network only)

Decoder Architecture:

- Hidden Layer(embedding-size+1, convoluted-size), BatchNorm, ReLU
- Hidden Layer(convoluted-size, 2*convoluted-size), BatchNorm, ReLU
- Hidden Layer(2*convoluted-size, 28*28), BatchNorm, Sigmoid