SIDEs: Separating Idealization from Deceptive ‘Explanations’ in xAI

EMILY SULLIVAN, Utrecht University, Netherlands

Explainable AI (xAI) methods are important for establishing trust in using black-box models. However, recent criticism has mounted against current xAI methods that they disagree, are necessarily false, and can be manipulated, which has started to undermine the deployment of black-box models. Rudin (2019) goes so far as to say that we should stop using black-box models altogether in high-stakes cases because xAI explanations ‘must be wrong’. However, strict fidelity to the truth is historically not a desideratum in science. Idealizations—the intentional distortions introduced to scientific theories and models—are commonplace in the natural sciences and are seen as a successful scientific tool. Thus, it is not falsehood qua falsehood that is the issue. In this paper, I outline the need for xAI research to engage in idealization evaluation. Drawing on the use of idealizations in the natural sciences and philosophy of science, I introduce a novel framework for evaluating whether xAI methods engage in successful idealizations or deceptive explanations (SIDEs). SIDEs evaluates whether the limitations of xAI methods, and the distortions that they introduce, can be part of a successful idealization or are indeed deceptive distortions as critics suggest. I discuss the role that existing research can play in idealization evaluation and where innovation is necessary. Through a qualitative analysis we find that leading feature importance methods and counterfactual explanations are subject to idealization failure and suggest remedies for ameliorating idealization failure.

CCS Concepts: • Computing methodologies → Machine learning; • Social and professional topics → Technology audits.

Additional Key Words and Phrases: explainable AI, idealization, philosophy of science, qualitative evaluation

ACM Reference Format:

1 INTRODUCTION

The ideal gas law dating back to 1834, along with its simpler cousin Boyle’s law from the 1660s, are still used to explain how gases behave. Boyle’s law captures the inverse relationship between pressure and volume at constant temperatures, which can explain why a balloon’s inflation level changes amidst elevation changes. The ideal gas law complicates the picture by adding the influence of temperature changes and molarity to gas behavior. However, both these laws involve distortions and departures from the truth [1, 2]. Real gases do not behave ideally. Particles are assumed not to interact (even though they do), and the actual relationship between pressure and volume is more complicated than either law lets on. Despite this, the ideal gas law is still highly successful—a highly successful idealization (i.e. an intentional distortion introduced to scientific theories and models).

Contrast this with a more controversial contemporary case. In 2021, RIVM, the Dutch health institute, constructed a model to measure the spread of nitrogen pollution. In order to reduce computational complexity, the model treated nitrogen deposits coming from roads as spreading only 5km, while the deposits from farms traveled much longer distances. However, this distortion—which idealization—was not a success, and was later removed because it disproportionately put the pollution blame on farms instead of highways [3]. What makes the ideal gas law a permissible, even

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2024 Copyright held by the owner/author(s).

Manuscript submitted to ACM
desirable, distortion, but the idealizations in the Dutch nitrogen model problematic, needing revision? It cannot simply be that the Dutch nitrogen model contains falsehoods vis a vis an idealization, or a lack of fidelity to the phenomena, since the ideal gas law does the same.

Now consider the topic at hand: explainable AI (xAI) methods. Rudin [4] argues that the increasing trend of using black-box ML models across science and society is problematic, precisely because the methods we use to interpret these models provide us with necessarily wrong explanations of how they work. Other recent works have painted a picture of mounting criticism that leading xAI techniques are unreliable, subject to manipulation, and different techniques often disagree [5–9]. Some critics argue that xAI is a ‘false hope’ [10], where methods can engage in explanation hacking [11] or fairwashing [12], leading users to unduly trust models [13–15], and more [16]. This raises the question: Do the falsehoods and approximations (i.e. idealizations) operating in xAI have the same secret of success as the ideal gas law? Or are the critics largely correct that current xAI methods need improvement before systematic deployment, like the Dutch nitrogen case? When are deviations from the truth successful idealizations? When are they deceptive distortions?

This paper seeks to animate a new research program for the study of xAI idealizations. Idealization evaluation moves beyond concepts of falsehood or model fidelity capturing a deeper issue: the norms and practices surrounding model limitations and their context of appropriate use. I introduce a broad evaluation framework for idealization evaluation in xAI that aims to separate successful idealizations from deceptive explanations (SIDEs) (sect. 4). I identify areas where existing xAI evaluation methods are useful for idealization evaluation, and where innovation is necessary. To build this framework, I first take inspiration from the idealization practices in the natural sciences (sect. 3). I take an off-the-shelf theory of idealization influential in philosophy of science, the minimalist view of idealization, and apply it to feature importance (sect. 4) and counterfactual explanation methods (sect. 5), showing through a qualitative analysis that idealization failure is common. Lastly, I consider ways of ameliorating idealization failure and point to future research directions for building a theory of idealization for xAI (sect. 6). It is also important to say what this paper does not do. It does not argue for a new philosophical theory of idealization or seek to diagnosis exactly what kind of idealization xAI methods engage in. Instead, I provide a modular framework for and show the potential for xAI researchers to engage with work on idealization in philosophy of science. The paper aims to make the following contributions:

(1) Conceptualizes the field of xAI as solving an idealization problem
(2) Introduces the SIDEs framework for evaluating idealizations in xAI, derived from normative foundations of idealization in the natural sciences and philosophy of science.
(3) Provides a theoretical grounding for novel evaluation methods for xAI.
(4) Identifies possible novel practices of idealization in xAI that needs normative analysis.

2 BACKGROUND AND RELATED WORK

The ever-growing fingerprint ML has on the production of scientific and social knowledge comes with challenges. One often cited issue is model opacity [17–19]. Transparency of ML decisions is important for building trust [14, 20–22], it might be legally required [23, 24], and convincing arguments have been made for a moral right to explanation in high-impact contexts [25]. This need for transparency inspired a proliferation of different interpretability and xAI techniques to solve the problem of opacity by providing insight into the reasons behind ML classifications. Post-hoc feature importance methods remain the most influential approach in xAI. These methods seek to approximate how much particular features contribute to the model’s decision locally around each prediction. Examples include LIME [26], SHAP which utilizes coalitions game theory [27], and saliency maps that visualize regions of interest [28, 29].
These methods differ from example-based or decision-rules [30], and differ from global explanation methods that seek to capture the behavior of a black-box system as a whole [31, 32]. However, there are ways to use LIME and SHAP to get close to a global explanation by aggregating many local explanations. Counterfactual explanation (CE) methods have recently gained notoriety as the leading alternative to feature importance methods [33–40]. CE methods seek to answer what-if-things-had-been-different questions by probing the ML model to see what minimal changes would reverse the ML decision. There are a variety of different algorithms for generating or filtering which counterfactuals would be relevant in different contexts and for different stakeholders (see [41] for a review). Despite these achievements there remain conceptual and evaluative challenges to xAI and explainability.

**Conceptual issues for xAI.** There are several conceptual contributions that philosophers of science have made in debates around xAI. Most notably, on the concept of explanation [21]. Central questions concern what type of information is required to fulfil the definition of an ‘explanation’ in philosophy of science [21, 42–45], such as conforming to a covering-law view of explanation [43] or having an additional link between the model and the world [46]. Others focus on ethical considerations regarding whether certain xAI methods can fulfil moral requirements for explanation [25, 33], such as a principled reason explanation [37]. These normative based approaches have exposed various challenges with xAI. For example, Symons and Alvarado [47] discuss the issue of epistemic injustice in the context of trying to solve ML opacity. Others have suggested that CE methods have the potential to hide bias [12, 37, 48, 49]. While even some argue that xAI methods are unnecessary and that model evaluation should focus instead on notions of reliability [50–53].

Discussions of the norms of explanation are no doubt important and necessary. However, as I hope to show in this paper, norms of explanation are distinct from the norms and ideals that govern idealization. However, only recently has there been a suggestion that the concept of idealization in xAI may be useful [54, 55]. Nevertheless, here researchers stop short of discussing how xAI researches could actually use idealization theory, and how we could evaluate idealizations.

**Current approaches to xAI evaluation.** Evaluating xAI methods in computer science include experimental methods, such as comparisons of accuracy and model fidelity between different algorithms and benchmarks [14, 56], whether methods are robust under manipulation or perturbations [5–7, 9], or whether such methods conform to human expectations [57–59]. Current evaluation methods have exposed a number of vulnerabilities. Accuracy tests conducted on feature importance methods, found that the best performing method only approached 85% agreement with the black-box model, with LIME often scoring lower [31]. Furthermore, feature importance methods were found to be vulnerable to adversarial manipulation. Slack et al. [5] were able to create explanations that hid the most salient feature for classification for SHAP and LIME. Ghorbani et al. [15] found such methods were highly sensitive to small changes to input data, with others finding that they are not able to capture causal notions [4, 14, 60]. Counterfactual explanation methods can also fall prey to manipulation. Specifically, it was found that hill-climbing CE methods can converge to different local minima resulting in possible manipulation [6]. They also suffer from the rashomon effect where different counterfactuals explaining the same decision can be contradictory [61, 62].

While current methods of xAI evaluation are no doubt insightful, important gaps remain. Current experimental methods actively look for vulnerabilities and look for cases where methods break down or where new methods show an improvement compared to benchmarks. However, they stop short of providing an analysis that evaluates whether the limitations and the distortions xAI methods introduce are actually problematic or could be a case of a successful idealization. Instead, several critics simply point to the existence of possible manipulation and limited model fidelity, as itself a strike against the method [4, 8, 9, 13, 14]. While others have argued that current notions of fidelity are ill-equipped to capture cases of misleading explanation [13, 56]. The potential for misleading explanations has also inspired
a user-centered approach to evaluation, where xAI evaluation is geared toward fulfilling either actual user preferences, or expected user perceptions of usefulness [20, 63, 64], including the introduction of normative stakeholder sensitive frameworks [65–69]. Again, while this evaluative approach is important, normative and theory-based evaluations concerning the potentially positive role a lack of model fidelity could have for xAI methods are lacking.

**Closing Gaps.** This paper aims to address the above gaps by introducing the concept and framework of idealization evaluation. While model auditing techniques look for vulnerabilities, idealization evaluation asks whether such vulnerabilities are problematic or actually a successful tool. Moreover, idealization evaluation provides the conceptual tools for identifying the fundamental goals for xAI more so than just looking at theories of explanation. With this paper, I hope to show the need for xAI research to build a theory of idealization and engage directly in idealization evaluation. Without a proper theory of idealization, it remains difficult to thoroughly diagnose the success of xAI methods. Idealization is inevitable, but if done right, idealization is desirable. My approach in this paper takes inspiration from idealization in the natural sciences and the philosophy of science to gain insight into how researchers can begin the project of idealization evaluation in xAI. I return to how idealization evaluation fits within current xAI research in section 4.

### 3 IDEALIZATION IN THE NATURAL SCIENCES AND PHILOSOPHY OF SCIENCE

Idealizations are the (intentional) distortion of real-world features that are present in a model or theory. In science idealizations are many. Examples include the ideal gas law and frictionless planes in physics, perfectly rational agents in economics, infinite populations and the absence of genetic drift in biology, etc. The way philosophers of science understand the concept of idealization might be best illustrated with an example outside of science. The Tube map of London’s underground has neatly organized lines, and the circle line resembles a circle. However, the Tube map distorts the actual layout of the Tube tunnels. In reality, the interconnection of tunnels is complex and rarely a straight line [70]. The official Tube map does more than leave out detail; it intentionally distorts the real layout of tunnel paths. The Tube map idealizes London’s subway structure. Philosophers of science have sought to understand and conceptualize the nature, function, and epistemic value of idealizations in scientific inquiry [2, 49, 71].

<table>
<thead>
<tr>
<th>Idealization Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>The purpose / function of the idealization (e.g. epistemic purpose, like understanding; ethical purpose, like recourse and contestability, etc.)</td>
</tr>
<tr>
<td><strong>Idealization Practice</strong></td>
<td>The set of scientific methods and practices that categorize a type of idealization, along with the justification of those practices (e.g. Minimalist idealization)</td>
</tr>
<tr>
<td><strong>Ideals</strong></td>
<td>Values and norms underlying an idealization practice and that govern rule development (e.g. causal-entailment, feasibility for users)</td>
</tr>
<tr>
<td><strong>Rules</strong></td>
<td>The way ideals are operationalized into a metric of evaluation</td>
</tr>
<tr>
<td><strong>User-facing explanations</strong></td>
<td>How idealizations are presented as explanations to end-users</td>
</tr>
</tbody>
</table>

**Features and types of idealization practices:** In a landmark paper in philosophy of science, Weisberg [72] proposed that idealizations should be categorized by their specific scientific practices made up of the activity of scientists, the
norms or values that govern these practices, and how these norms are justified. We can translate these aspects of idealization into three features (idealization practice, ideals, rules) that are important in the natural sciences, adding two additional features for xAI (See Table 1). Philosophers of science have conceptualized several different idealization practices in the natural sciences, like the unique quality of infinite idealizations [73] and asymptotic idealizations in physics [74, 75], hypothetical-pattern idealization in biology [76], the practice of Galilean idealization, multiple-model idealization [72], and more. In this paper, we restrict discussion to one influential theory of idealization, Streven’s [77, 78] minimalist view of idealization (MinI). Below I will discuss how MinI works in a simple physics case, and in the next section discuss why MinI resembles the idealization practices in xAI and is a good place to start for evaluating xAI’s idealizations. In section 6, I discuss alternative idealization practices that xAI could be engaged in.

Minimalist idealization in physics. The underlying norm for MinI is that simple models and explanations are better than more complex ones. Understanding phenomena requires isolating relevance from irrelevance often requiring idealization. MinI’s idealization practice consists of devising scientific (or mathematical) methods for reducing the number of features that give rise to a phenomenon, highlighting the difference-makers, and only distorting the non-difference-makers. As such, the governing ideals for MinI are simplicity and isolating difference-makers [77, 78]. In physics, relevance and difference-making is usually a type of causal or dependency entailment, where some causal consequence can be (logically) derived from a set of initial conditions along with a causal law. In cases where the law is non-causal, the entailment is a different type of dependency entailment (such as a mathematical dependency) [79]. While Streven [77] focuses on causal difference-making, others have adopted non-causal approaches to MinI [80].

The most discussed example of MinI is the ideal gas law. The ideal gas law introduces the false assumption that a system consists of $N$ non-interacting particles so that physicists can clearly see that phase space is proportional to volume. The justification for adding the idealization of non-interacting particles is that in contexts of low pressure and high temperature, particle interactions are virtually insignificant to the relations between pressure, temperature, molarity, and volume. The idealization highlights this irrelevancy in a way that a more accurate representation hides.

However, if we remove the idealization, we can still determine the irrelevance of particle interactions. We can derive the virial equation of state directly from statistical mechanics with arbitrary precision by extending the equation indefinitely, where each added term is derived from an increasingly detailed and accurate representation. However, the contribution of each added term becomes vanishingly small, again resulting in the ideal gas law [49]. Thus, the ideal gas law satisfies the inclusion and fidelity rules of MinI by only removing and distorting aspects that do not affect causal-entailment (i.e. only distorting non-difference-makers). In cases where entailment fails and the ideal gas law does not capture gas behavior (e.g. in high pressure), other laws are required (e.g. Van der Waals). Importantlly, even if it is possible to de-idealize in this case, MinI is still appropriate. MinI captures the difference-makers that a more accurate alternative does not. As such, idealized distortions are permanent fixtures—even if they can in principle be removed—because they distinguish relevance from irrelevance.

Idealization in xAI?. Machine learning is not the type of practice that philosophers of science have built their idealization theories around. ML models are complex instead of simple and they are not constructed with built-in theoretical assumptions where model equations explicitly represent processes in the target system [81]. ML models are often used precisely because such theoretical assumptions are unavailable, or because researchers are interested in prediction or overlooked patterns of interest. Moreover, in the case of xAI, the xAI model is an idealization not of the world but another model (the ML model). Thus, we need to separate between two questions of xAI and ML idealizations:
- **Model-World question**: How do black-box ML models idealize some real-world phenomenon? (e.g. how do ML models idealize aspects of disease indicators?) [46, 82, 83]

- **Model-Model question**: How do xAI methods idealize how a black-box ML model works? How is an xAI method an idealized representation of the black-box model? (e.g. how do feature importance methods idealize aspects of the ML model decision process?)

XAI mainly concerns the Model-Model question (we return to Model-World questions for xAI in sect. 5). Like the ideal gas law, there are several similarities between the xAI project and MinI. Current work in xAI often describes the ultimate goal of xAI methods as uncovering how black-box models make decisions, capturing how various inputs can cause a particular output in the black-box model [21, 60, 84]. This leaves Fleisher [55] to argue that feature importance methods are a kind of MinI because they satisfy simplification, flag difference-makers, and focus on a specific causal pattern in the black-box model that gives rise to the decision (i.e. answering the Model-Model question). For example, LIME uses linear approximation methods that distort aspects of the black-box model decision making process, but does so by aiming to find the features that are the central difference-makers for a given local decision (e.g. high debt is the largest difference-maker for why the black-box model recommended loan rejection). But are feature importance successfully engaging in MinI, like the ideal gas law?

4 **TOWARD A FRAMEWORK FOR IDEALIZATION EVALUATION IN XAI**

In this section, I introduce the SIDEs framework. SIDEs consists of a high-level modular workflow (Figure 1) that can guide researchers with key questions for reflection and qualitative evaluation of xAI idealizations. I go through each phase of SIDEs, identifying areas where existing theories and experimental evaluation techniques are useful and where innovation is required. If idealizations meet the standards for each phase, with alignment between phases, then the idealization is successful. Idealization failure occurs when there is misalignment or the idealization fails to meet the standards for a given phase. Throughout this section, leading feature importance methods, LIME and SHAP, are qualitatively evaluated to illustrate how SIDEs can identify risks of idealization failure. In section 5 I turn to CE methods.

![Fig. 1. SIDEs Workflow](image)

4.1 **Purpose**

In philosophy of science idealization analysis begins with an idealization practice. However, xAI calls for starting idealization analysis with the purposes that researchers are aiming to achieve with idealizations [85]. In the natural sciences, idealizations are discussed in the context of ideal scientific agents, so the central purpose of an idealization is presupposed to be epistemic by enabling understanding of phenomena [1, 86]. However, xAI methods serve a variety of
purposes beyond epistemic purposes, including ethical purposes like recourse, where the aim is informing end-users about actionable changes that could reverse a negative decision [39]. To capture this difference, the SIDEs workflow starts with identifying the overall purpose the xAI method serves in a given context.

I want to highlight two potentially conflicting purposes of xAI methods: epistemic and ethical purposes. However, additional purposes are possible (e.g. legal compliance). While it can be helpful to discuss purposes of xAI broadly, finer grained aims are more useful for idealization evaluation. For example, fine-grained epistemic purposes could be understanding the phenomena the model bears on [46], predictive knowledge [87], user-specific epistemic goals [88], and more [89, 90]. Ethical purposes include fairness [91], providing users with recourse (i.e. actionable interventions) [33], exposing model bias, etc. Purposes are not necessarily mutually exclusive and may overlap. A single xAI explanation might aim to satisfy several purposes at once, such as providing users understanding of the model and building users’ trust in the model, while also providing a user with algorithmic recourse. SIDEs does not preclude xAI methods from serving multiple purposes; however, the bar for successful idealization could become considerably higher (see section 5).

4.1.1 Evaluating Purpose. The purpose phase in SIDEs asks researchers to reflect on what purposes an xAI method does and should have in a specific context. There are several existing works that have identified various purposes that xAI methods serve [14, 92], and there is normative and theory-based work on xAI concerning what purposes xAI should have that can be helpful for evaluating purpose [68]. A central pitfall for xAI methods is the risk of idealization failure due to misalignment with purpose. For example, in the original LIME paper, Ribeiro et al. [26] describe the motivating purpose behind LIME as establishing user trust. However, trust could have divergent underlying aims. On the one hand, trust can serve an ethical purpose. In clinical cases, patients trust of a doctor’s diagnosis is often not grounded in the patient’s knowledge or understanding of the diagnosis [93, 94]. On the other hand, there are other contexts where trust is only achieved when users understand the reasoning behind decisions. This tension between different functions of trust complicates the picture of whether an xAI method engages in idealizations that could fulfill these various purposes. For example, Lakkaraju and Bastani [13] found LIME is able to manipulate user trust.

4.1.2 Role and limits of current work. Current research directions in xAI are well-placed to evaluate the purposes that xAI methods do and should have, with significant work already being done [14, 20, 45, 85, 92]. Re-conceptualizing xAI as an idealization problem relies on this work as the first fundamental step toward establishing how model fidelity should be understood and which features of black-box models can be distorted (i.e. idealized). Idealization evaluation asks researchers when analyzing purposes of xAI to consider the extent to which model fidelity matters.

Key questions for the purpose phase are:

- What purpose does an xAI explanation have in a particular context? What purpose should it have?
- What aspects of the model need to be known for a particular purpose?
- **Example**: What notion of trust is an explanation aiming for in a particular context?
- **Success**: The purpose of the xAI explanation is appropriate for the given deployment context.

4.2 Idealization practices

As discussed in section 3, idealization practices consist of the set of scientific methods and practices along with the justification of those practices. One central research area in philosophy of science is conceptualizing different idealization practices across the sciences into distinguishable types or theories of idealization.
4.2.1 Evaluating Idealization Practices. Evaluating the idealization practices phase involves two central aspects. The first is a descriptive project that systematizes current work in xAI, elucidating a set of common aims and methodologies. This can be done for xAI in general or for a specific class of xAI methods. Second, evaluating idealization practices consists of a justification step that can ground the legitimacy of the idealization practice. Using MinI as our working hypothesis, the methodology of MinI consists in omitting or distorting (causal) influences for the purposes of highlighting the central (causal) difference-makers or (causal) patterns. MinI is justified both through a strong conceptual foundations in scientific understanding, explanation, and (causal) difference-making, and in its empirical success [71].

4.2.2 Role and limits of current work. Currently there has been very little work trying to conceptualize the type of idealization practices computer scientists are engaged in when developing xAI methods [55], and these practices are still arguably elusive [14]. However, as discussed in sect. 3, there are several similarities between current xAI methods and MinI. XAI aims to cut through the noise of many feature interactions to arrive at the chief difference-makers for a decision. For the purposes of this paper, we evaluate xAI methods as if they are engaging in the idealization practice of MinI. However, this paper calls for xAI to actively engage in solidifying one or more idealization practices and to work with philosophers of science on establishing conceptual foundations that justify these idealization practices. This is a central area that requires innovation and future research (see also section 6).

Key questions for the idealization practices phase are:

- What are the specific methods of deriving idealizations (e.g. introducing certain idealization assumptions, mathematical operations applied on data that results in distortions of the phenomena)?
- Does the idealization practice align with the purpose of the idealized model?
- What justifies this particular idealization practice? Why is it suitable for the identified purpose?
- Example: Minimalist idealization provides better understanding of the relevant difference-makers.
- Success: The idealization practice is well-grounded and justified in a specific domain, aligning with purpose.

4.3 Ideals and Rules

Ideals are the norms and values that govern a specific idealization practice. Rules are the operationalization of these norms and values. For example, the ideals for MinI are to isolate the minimum number of difference-makers that capture a phenomenon, while Strevens [77] describes the fidelity and inclusion rules of MinI as satisfying a ‘causal entailment’ test, where modelers remove (or distort) features, finding the minimal amount that still entail the desired event.

4.3.1 Evaluating ideals and rules. Evaluating idealizations in the ideals and rules phase requires validating whether specific rules embody target ideals, and analyzing trade-offs between different ways of operationalizing ideals. Idealizations can be experimentally validated by developing tests that satisfy these rules. Adopting our working hypothesis that xAI is engaging in MinI means that for xAI methods to be a legitimate idealization of a black-box model and pass the ideals and rules phase, xAI methods must isolate the difference-makers for the target black-box model’s decision by undergoing a (causal) entailment test that ensures the xAI method gives the same results as the target black-box model. Passing an entailment test would mean, in theory, that the xAI method uncovers the minimum set of difference-makers that determine the black-box model’s decision [84], and thus any distortion it makes in the process is a legitimate one.

However, specifying an adequate (causal) entailment test is not simple. First, the notion of difference-making in xAI must be clear. For Strevens [77, 78], MinI aims for causal difference-making, where the notion of causality is left implicit and entailment more closely resembles logical deduction. Comparatively, philosophical theories like an
interventionist framework [84, 95] or a counterfactual framework [96, 97] would result in grounding different causal rules. Alternatively, MinI need not aim for causal difference-making at all; other notions of difference-making are consistent with MinI (logical, probabilistic, mathematical, etc.). Thus, it is necessary to establish the specific ideals that a given idealization seeks to capture. Second, even once we settle on a notion of difference-making for MinI, there are still different possible rules that could capture the norms of MinI and serve as a basis for idealization evaluation. In this section, I consider three possible rules based on Strevens view of MinI. My aims are to 1) illustrate how ideals might be operationalized (see Table 2); 2) discuss how to think about trade-offs and whether a certain rule embodies the target ideal; and 3) discuss where existing evaluation methods in xAI are useful and areas where innovation is needed.

<table>
<thead>
<tr>
<th>Table 2. Entailment rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP</td>
</tr>
<tr>
<td>∀x b(x) = e(x)</td>
</tr>
</tbody>
</table>

First, MinI entailment could be a global entailment where the xAI model shares the same mapping of model inputs to outputs as the black-box model. The MAP rule requires that the mapping of inputs and outputs for an xAI model, e, is the same as for the black-box model, b. MAP does not look at the features that the xAI model highlighted as relevant. As long as there is a 1 to 1 input-output mapping, then this is enough to establish a global notion of (causal) entailment. MAP aligns with some of the current approaches to xAI evaluation. Accuracy and model fidelity metrics used for feature importance methods aim to see how well explanations mirror black-box predictions [13]. The results of these tests have exposed important vulnerabilities. For example, Lakkaraju et al. [31] found the best performing method only approached 85% agreement with the black-box model, with LIME often scoring lower. Even if we have a 1-1 mapping, an important trade-off to consider with MAP is how well it aligns with the purpose for xAI. Usually the purpose of an xAI method is for users to learn about the reasons for why the black-box model made its decision, not merely that an alternative proxy-model (in the case of LIME and SHAP) can derive the same predictions, which is why Lakkaraju et al. [31] argue that high-fidelity xAI models aren’t enough.

Second, as an alternative, we could operationalize entailment more closely with Strevens’ [77] own elimination test for MinI in the natural sciences. ELIMINATION tells us that for all the features Y that are in the set of putatively irrelevant features I found from the xAI model e, we can remove those features from the set of all input features X from the black-box model b and still receive the same decision. According to ELIMINATION, evaluation could occur for any given local decision to see whether in that instance there is entailment between the black-box model and the xAI model. As we saw, one general downside of MAP is that an input-output pairing does not capture which features xAI methods determine are (ir)relevant ELIMINATION captures this aspect of explainability. Since ELIMINATION can be evaluated per local decision, there is more flexibility for success. Some local decisions may not satisfy ELIMINATION, while others do. Indeed, in the cases where the xAI method works well, ELIMINATION should be satisfied. But the trade-off here is that idealization failure would needs to be tested for each local decision.

Lastly, as yet another alternative, some philosophers of science have argued only a probabilistic notion of (causal) relevance or difference-making is necessary for MinI [98]. PROB can apply to any other rule. It says that the probability that a rule applies to x is greater than some probability threshold t. That said, PROB may not align well with the ideals for MinI for many xAI purposes, for example users may not want to know what the most probable reason for the decision was, but the actual reason for the decision. However, when using xAI for the purposes of de-bugging or de-biasing a black-box model, PROB could be appropriate.
4.3.2 Role and Limits of Current Work. The ideals and rules phase is the area in xAI idealization evaluation that requires innovation. In philosophy, Fleisher [55] argues feature importance methods are a kind of MinI, but he argues this on the level of ideals and stops short of discussing whether particular xAI methods actually succeed at MinI instead of merely aiming for MinI. Other works focus on the norms and ideals of explanations for xAI. Citing one example, Watson et al. [63] propose the ideal of sufficiency for xAI methods because they provide potentially more useful and ‘lower cost’ explanations for users. However, the norms and ideals for explanation are distinct from the norms and ideals that govern idealization evaluation. Idealization evaluation, first and foremost, treats xAI models not as explanation tools, but as idealized models of more complex models. SIDEs evaluates whether the distortions a given xAI method engages in succeeds at living up to the purpose and norms of idealization theory.

On the level of rules, there are existing experimental techniques that have been used to evaluate LIME and SHAP that capture some of the spirit of our suggested entailment rules for MinI, like map discussed above. While LIME and SHAP do not satisfy map because the accuracy rates do not reach perfect alignment between the black-box model and the xAI model, map’s prob counterpart has some level of success depending on the probability threshold. However, even a .8 probability may be too low to establish a strong sense of causal entailment for MinI. So if the ideal for xAI is a causal ideal then there is still idealization failure in the leading feature importance methods. There is no experimental test that captures elimination that I am aware of. However, feature importance methods are vulnerable to adversarial manipulation. Slack et al. [5] were able to create explanations that hid the most salient feature for classification for SHAP and LIME. Ghorbani et al. [15] found such methods were highly sensitive to small changes input data. Others have found that they are not able to capture causal notions [4, 14, 60]. This type of manipulation suggests that feature importance methods are not robustly conforming to elimination. Moreover, adversarial examples where the adversarial classifier achieves strong prob(map) but the perturbed instances are different (see [5]) shows the tension between more global oriented rules like map and local entailment rules like elimination. This suggests that in order to fully capture MinI, it may be necessary to satisfy both map and elimination.

Innovation on new experimental evaluations that instantiate idealization rules could be promising. In this paper, I took just one conception of (causal) entailment from Strevens to ground potentially new experimental evaluation tests for xAI. XAI researchers should consider the idealization norms and ideals they are aiming to achieve and align experimental evaluation tests with these norms. Existing theories of idealization in philosophy of science could serve as inspiration for establishing quantitative evaluation metrics for idealization.

Key questions for the ideals and rule phase are:

- **What are the norms and values that govern and justify an idealization practice?**
- **What are the possible ways to operationalize ideals to experimentally and formally evaluate whether an idealized model satisfies the ideals of the idealization practice?**
- **What are the trade offs between different rules?**
- **Example:** Different possible entailment rules for MinI and the limitations of each.
- **Success:** Rules adequately reflect ideals. The xAI method satisfies the rule by passing an experimental test.

4.4 User-facing explanations

Work on idealization in the natural sciences considers scientists as stakeholders. The ideal gas law idealization is successful mainly because the intended audience generally knows enough about physics to understand where the idealizations lie. XAI, on the other hand, serves many diverse stakeholders, many of which do not know how ML works
in any detail. Therefore, attention must be paid to the way idealizations are presented to different stakeholders through user-facing explanations. Thus, the last step for the SIDEs framework is evaluating user-facing explanations.

### 4.4.1 Evaluating user-facing explanations

Evaluating the explanations that target users receive involves user testing and user studies to ensure that explanations align with purpose and do not mislead users with its idealizations. One general pitfall for aligning user-facing explanations with user values is the potential for ‘explanation hacking’ where xAI methods are so flexible to display only those that are agreeable to users [11], which can result in fairwashing [12]. Even if the xAI method is a successful idealization from a scientific or mathematical perspective (i.e. passes the rule phase), there can be idealization failure if it misleads users through explanation hacking or fairwashing techniques. Moreover, Mittelstadt et al. [58] found that users found LIME and SHAP unintuitive. Other considerations include doing user-study research not just for experts, but for a variety of users that have different background assumptions [99]. Including users from the global south, which are often ignored [100, 101].

### 4.4.2 Role and Limits of Current Work

Several existing works address issues regarding user-facing xAI. Some provide frameworks that incorporate stakeholder interests [65–69], others explore how different explanation types affect user-trust [20], cognitive bias [102, 103], and understanding [38, 104]. SIDEs adds to this by highlighting the need for user-facing explanations to align with the purpose of idealizations, conveying the ideals and norms of the idealizations in the explanations they receive. For example Schneider and Vlachos [105], used language similar to MinI when describing the results of their user study, saying that users could tease out what was relevant and irrelevant to a model decision.

Key questions for the user-facing explanation phase are:

- Do users understand the purpose of the explanation?
- How can user-facing explanations convey that the explanation is an idealization?
- Are user-facing explanations evaluated in terms of the purpose? Are they evaluated in terms of another purpose?
- Example: A user study asks users about their impressions regarding the purpose and limits to the explanation.
- Success: User-facing explanations align with purpose and users acknowledge the limited scope of explanations.

## 5 EVALUATING COUNTERFACTUAL EXPLANATION METHODS

In the previous section, I introduced the SIDEs framework and presented a qualitative evaluation of leading feature importance methods, LIME and SHAP. In this section, I identify risks of idealization failure in counterfactual explanation (CE) methods, using SIDEs. It is important to note that proponents of CE methods boast that CE cannot be false since counterfactuals are generated from the black-box model itself [38]. However, such methods still engage in idealization. CE methods must select which counterfactual scenarios are the most salient from a larger set of possible counterfactuals and implicitly rely on notions of difference-making that seek to tease out the relevant counterfactual scenarios from the less relevant. This is one reason why it is important to re-conceptualize xAI as seeking to solve an idealization problem, instead of the current frame of xAI aiming at ‘faithful’ explanations.

### Misalignment in CE:

Wachter et al. [34] highlight three different purposes for counterfactual explanation methods: i) explain why a decision was reached, ii) provide grounds to contest the decision, and iii) provide users with actionable changes to reverse the decision. SIDEs first requires that the idealizations used align with each specific purpose. i) has a clear epistemic purpose aimed at gaining understanding of the black-box model behavior, while using CE for iii)–known as recourse–has gained considerable attention regarding its ethical promise [33, 48]. A recourse explanation is one where users are given feasible actions for them to undertake to reverse a model decision (e.g. paying down
existing debt to qualify for a loan). Importantly, recourse and purely epistemic explanatory aims come apart \[11, 106\]. Since recourse provides users with actionable changes that they can make to reverse a decision, recourse explanations can mask bias and principle-reason explanations \[37\]. It could be that an immutable feature, like gender or race, was the biggest difference-maker for why the model made its decision. Such an explanation cannot, in principle, be a recourse explanation. This is one reason why Sullivan and Verreault-Julien \[48\] suggest conceptualizing recourse as a recommendation to avoid misleading users.

The type of idealizations that can satisfy MinI for understanding the decision do not immediately translate to idealizations that are acceptable if the purpose of the idealization is to provide users with recourse. For example, for the epistemic purpose of understanding, CE methods can idealize and distort the underlying causal structure in the data and idealize away any interdependence between features—especially if the underlying black-box model ignores interdependence between features. In the epistemic case, satisfying MinI only requires alignment between the xAI model and the black-box model (i.e. answering the model-model question). However, recourse explanations have a different target: the relationship between model features and the world \[41\], thereby aiming to answer a model-world question. For recourse, an idealization that ignores feature interdependence and the underlying causal structure in data will likely fail MinI rules that are calibrated to capture aspects of real-world causal efficacy. Indeed, works have criticised CE methods that ignore feature interdependence as creating unrealistic advice \[107\].

Fig. 2. Recourse Alignment Failure

Purpose-alignment-failure can carry over to how xAI explanations are conveyed to users in the user-facing explanation phase. For example, recourse explanations are often presented as answering a model-model question (i.e. understanding of how the black-box model behaves), with several works evaluating their recourse method on whether users have similar understanding of the models decision boundary compared to, e.g. LIME \[34, 38, 39\]. However, since the underlying purposes of recourse CE are feasibility and actionability, evaluating recourse CE should be done in terms of whether users find the recourse CE feasible. Understanding the model’s decision is secondary. Figure 2 shows this type of recourse CE alignment failure, where the explanation is evaluated based on the wrong purpose. This is not to say that recourse explanations could not be successful idealizations. SIDEs maintains that omitting or distorting the central reasons for a model’s decision from a recourse explanation is legitimate so long as the user-facing explanation is aligned with actionability, while making clear to the user it is not an epistemic explanation. Of course, it is possible that CE could satisfy both an epistemic purpose and recourse. However, for an idealization to achieve both aims there is a considerably higher bar where the CE method would need to satisfy both difference-making w.r.t. the model-model question and difference-making w.r.t. the model-world question. We should expect that this might be possible in some cases, but not likely in cases where immutable features are the largest difference-maker for a model’s decision.

Ideal and rule failure. Many of the same issues that come up with rule evaluation for feature importance methods also appear with CE methods. However, like the alignment issues discussed above, recourse CE has unique
risks. The governing ideals for recourse are feasibility and actionability. Thus, a structural causal model (SCM) that captures how features within a model causally dependent on each other [108–110] will be necessary to satisfy MinI, albeit an idealized SCM. However, SCMs are far from attainable, requiring a link to the causal realities outside of the model [46, 110]. Thus, the purpose of recourse, coupled with the idealization practice MinI, requires a causal rule that can uphold the ideal of a SCM. However, Karimi et al. [41] find most works on recourse do not even aim for a SCM. Thus, these methods are engaging in idealization failure. Karimi et al. [111], on the other hand, employ a probabilistic approach to try and capture the ideal of a SCM with imperfect causal knowledge, and thus is a candidate for a \textsc{prob(scmm)} rule, and might indeed be an idealization success, depending on how the \textsc{prob(scmm)} rule isolates difference-makers.

All told, researchers need to be mindful that model-world questions and model-model questions require different idealizations and have different idealization standards.

6 TURNING IDEALIZATION FAILURE INTO SUCCESS

In our limited evaluation of feature importance and CE methods we found that on the working hypothesis that xAl methods are aiming for MinI there is widespread idealization failure, due to misalignment with purpose and rule failure, suggesting that these methods may likely distort more than just the non-difference-makers. Where does this leave us? In this section I discuss possible remedies for idealization failure and areas for future research.

Adopting a different idealization practice: If it is too difficult to satisfy one idealization practice, such as MinI, then idealization success can occur by creating alignment with a different idealization practice. Rule failure under one idealization practice does not entail rule failure under another. Figure 3 shows realignment with a different idealization practice after rule failure. As we said at the outset there are a number of idealization practices that philosophers of science have discussed. One alternative idealization practice that may be well suited for xAI is multiple-model idealization (MMI) [72]. For some phenomena there may be several trade-offs that makes it either impractical or epistemically lacking to rely on just one model. MMI involves multiple models, with each model capturing one aspect or trade-off for some phenomenon. For example, chemists use both valence bond and molecular orbital models despite their incompatible assumptions [72]. The underlying justification for MMI relies on the impossibility (either practically or necessarily) of a single model capturing maximal goals of representation, such as accuracy and generality [112]. Furthermore, through robustness techniques among multiple models, MMI teases out relevance from irrelevance, something that MinI might fail to achieve in a single model [113]. While each individual model in the MMI might have drawbacks, the collection of models taken together is able to provide understanding.

![Fig. 3. Adopting an alternative idealization practice to address rule failure](image)

One notable solution to the idealization failure with MinI is to use LIME, SHAP and CE as part of a MMI instead. Realigning to MMI means that the rules for each xAI method can be less demanding. Each model, fulfilling a different
ideal or rule explores different trade-offs, together capturing how a black-box model makes decisions. Moreover, MMI can be a temporary solution to xAI manipulation. Slack et al. [5] found that adversarial attacks designed for LIME were ineffective against SHAP. Even though they also found that adversarial attacks designed against SHAP affected LIME, if the MMI also includes CE methods (or other methods) the vulnerability that each will be affected by the same attack diminishes. Furthermore, MMI can help with the problem of multi-purposes for xAI models. Users can be provided multiple explanations to fulfil these multiple purposes. However, MMI is not an simple fix. First, it is important to develop an aggregation rule for MMI idealizations. How should we weigh the different and sometimes conflicting models? This is a considerable undertaking. Second, current work has discussed that providing users with multiple different explanations can be counter-productive, creating confusion and cognitive overload [114]. Thus, MMI might not be a useful idealization practice outside of an engineering model-auditing setting.

**xAI, a novel idealization practice?** In this paper, we looked at mature theories of idealization from the philosophy of science that were developed with the natural sciences in mind. It would not be surprising if those theories are altogether ill-suited for xAI since xAI and ML research has very different and specific requirements compared to the natural sciences. For example, one unique aspect of many xAI methods are their hyper locality. In the natural sciences, idealizations often move away from local particulars to more global generalities. But current methods of xAI are distorting the global generalities of the black-box model to zoom in on a particular local explanation. Perhaps this is a novel hasty generalization idealization practice. One area for future research is developing what this potentially novel idealization practice consists of and how it might be justified and grounded as a legitimate idealization practice. Importantly, the SIDEs framework cautions against idealization success simply by fiat (i.e. by claiming a new idealization practice). SIDEs requires a justification step for motivating why such a practice is legitimate.

7 CONCLUSION

XAI methods have received their fair share of criticism. However, with this paper I argued that one type of criticism–that xAI methods produce false explanations of black-box models–deserves closer attention. Specifically, this paper seeks to animate a new interdisciplinary research program in xAI that develops a theory of xAI idealizations and idealization evaluation. It is not simply departure from the truth that is problematic, but idealization failure. I introduced the SIDEs framework as a way for researchers to separate successful idealizations from deceptive explanations. SIDEs is a generalizable and modular conceptual framework that can guide researchers with key questions for reflection and qualitative evaluation, as well as provide the normative foundation for developing more concrete evaluative tests and benchmarks for xAI methods. SIDEs is primarily aimed at xAI researchers when developing and evaluating their methods (esp. the ideals and rules phase). However, there is also a place for SIDEs in more downstream uses. Those who deploy xAI models could use SIDEs in selecting which xAI method would be more successful for their purpose, such as providing recourse explanations vs. model auditing. However, this would require clear guidance on the results of the rest of the SIDEs workflow from xAI researchers. Moreover, the user-facing explanation phase could be useful for thinking about how to comply with the right to explanation in AI governance.

Using SIDEs, we found considerable risks of idealization with leading xAI methods. There are many ways in which current work in xAI is useful for idealization evaluation, such as identifying the purpose of xAI methods, developing user-centered studies to evaluate the efficacy of explanations. However, there are central ways in which innovation is necessary: 1) identifying and solidifying an idealization practice for xAI, including a justification for that practice, and 2) developing experimental tests that aim at evaluating how well an xAI method idealizes the target black-box model.
ACKNOWLEDGEMENTS

For helpful comments and discussions I’d like to thank Céline Budding, Thomas Grote, Yei Streppel, Philippe Verreault-Julien, Carlos Zednik, with special thanks to John Mumma. I presented this work in various stages in development at the Munich Center for Mathematical Philosophy, University of Tübingen, Utrecht University, and Nicolaus Copernicus University. I thank those in attendance for the fruitful discussions that followed. This work is supported by the Netherlands Organization for Scientific Research (NWO grant number VI.Veni.201F.051).

REFERENCES

[14] Zachary C Lipton. The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. *Queue*, 16(3):31–57, 2018.


