Toward Causal Representation Learning

By Bernhard Schölkopf, Francesco Locatello, Stefan Bauer, Nan Rosemary Ke, Nal Kalchbrenner, Anirudh Goyal, and Yoshua Bengio

ABSTRACT | The two fields of machine learning and graphical causality arose and are developed separately. However, there is, now, cross-pollination and increasing interest in both fields to benefit from the advances of the other. In this article, we review fundamental concepts of causal inference and relate them to crucial open problems of machine learning, including transfer and generalization, thereby assaying how causality can contribute to modern machine learning research. This also applies in the opposite direction: we note that most work in causality starts from the premise that the causal variables are given. A central problem for AI and causality is, thus, causal representation learning, that is, the discovery of high-level causal variables from low-level observations. Finally, we delineate some implications of causality for machine learning and propose key research areas at the intersection of both communities.

KEYWORDS | Artificial intelligence; causality; deep learning; representation learning.

I. INTRODUCTION

If we compare what machine learning can do to what animals accomplish, we observe that the former is rather limited at some crucial feats where natural intelligence excels. These include transfer to new problems and any form of generalization that is not from one data point to the next (sampled from the same distribution), but rather from one problem to the next—both have been termed generalization, but the latter is a much harder form thereof, sometimes referred to as horizontal, strong, or out-of-distribution generalization. This shortcoming is not too surprising, given that machine learning often disregards information that animals use heavily: interventions in the world, domain shifts, and temporal structure—by and large, we consider these factors a nuisance and try to engineer them away. In accordance with this, the majority of current successes of machine learning boil down to large-scale pattern recognition on suitably collected independent and identically distributed (i.i.d.) data.

To illustrate the implications of this choice and its relation to causal models, we start by highlighting key research challenges.

A. Issue 1—Robustness

With the widespread adoption of deep learning approaches in computer vision [103], [140], natural language processing [55], and speech recognition [86], a substantial body of literature explored the robustness of the prediction of state-of-the-art deep neural network architectures. The underlying motivation originates from the fact that, in the real world, there is often little control over the distribution from which the data come from. In computer vision [76], [228], changes in the test distribution may, for instance, come from aberrations, such as camera blur, noise, or compression quality [107], [129], [170], [206], or from shifts, rotations, or viewpoints [7],...
Motivated by this, new benchmarks were proposed to specifically test a generalization of classification and detection methods with respect to simple algorithmically generated interventions, such as spatial shifts, blur, changes in brightness or contrast [107], [170], time consistency [95], [227], control over background and rotation [12], as well as images collected in multiple environments [20]. Studying the failure modes of deep neural networks from simple interventions has the potential to lead to insights into the inductive biases of state-of-the-art architectures. So far, there has been no definitive consensus on how to solve these problems, although progress has been made using data augmentation, pretraining, self-supervision, and architectures with suitable inductive biases with respect to a perturbation of interest [60], [64], [137], [170], [206], [233]. It has been argued [188] that such fixes may not be sufficient, and generalizing well outside the i.i.d. setting requires learning not mere statistical associations between variables, but an underlying causal model. The latter contains the mechanisms giving rise to the observed statistical dependences and allows to model distribution shifts through the notion of interventions [35], [180], [183], [188], [220], [237].

B. Issue 2—Learning Reusable Mechanisms

Infants’ understanding of physics relies upon objects that can be tracked over time and behave consistently [53], [236]. Such a representation allows children to quickly learn new tasks as their knowledge and intuitive understanding of physics can be reused [17], [53], [144], [250]. Similarly, intelligent agents that robustly solve real-world tasks need to reuse and repurpose their knowledge and skills in novel scenarios. Machine learning models that incorporate or learn structural knowledge of an environment have been shown to be more efficient and generalize better [9], [11], [15], [16], [27], [58], [77], [84], [85], [141], [157], [177], [181], [197], [211], [212], [244], [258], [272], [274]. In a modular representation of the world where the modules correspond to physical causal mechanisms, many modules can be expected to behave similarly across different tasks and environments. An agent facing a new environment or task may thus only need to adapt a few modules in its internal representation of the world [85], [219]. When learning a causal model, one should, thus, require fewer examples to adapt as most knowledge, that is, modules, can be reused without further training.

C. Causality Perspective

Causation is a subtle concept that cannot be fully described using the language of Boolean logic [151] or that of probabilistic inference; it requires the additional notion of intervention [183], [237]. The manipulative definition of causation [118], [183], [237] focuses on the fact that conditional probabilities (“seeing people with open umbrellas suggests that it is raining”) cannot reliably predict the outcome of active intervention (“closing umbrellas does not stop the rain”). Causal relations can also be viewed as the components of reasoning chains [151] that provide predictions for situations that are very far from the observed distribution and may even remain purely hypothetical [163], [183] or require conscious deliberation [128]. In that sense, discovering causal relations means acquiring robust knowledge that holds beyond the support of observed data distribution and a set of training tasks, and it extends to situations involving forms of reasoning.

Our contributions: In this article, we argue that causality, with its focus on representing structural knowledge about the data generating process that allows interventions and changes, can contribute toward understanding and resolving some limitations of current machine learning methods. This would take the field a step closer to a form of artificial intelligence that involves thinking in the sense of Konrad Lorenz, that is, acting in an imagined space [163]. Despite its success, statistical learning provides a rather superficial description of reality that only holds when the experimental conditions are fixed. Instead, the field of causal learning seeks to model the effect of interventions and distribution changes with a combination of data-driven learning and assumptions not already included in the statistical description of a system. This work reviews and synthesizes key contributions that have been made to this end.

1) We describe different levels of modeling in physical systems in Section II and present the differences between causal and statistical models in Section III. We do so not only in terms of modeling abilities, but also discuss the assumptions and challenges involved.

2) We expand on the independent causal mechanism (ICM) principle as a key component that enables the estimation of causal relations from data in Section IV. In particular, we state the sparse mechanism shift (SMS) hypothesis as a consequence of the ICM principle and discuss its implications for learning causal models.

3) We review existing approaches to learn causal relations from appropriate descriptors (or features) in Section V. We cover both classical approaches and modern reinterpretations based on deep neural networks, with a focus on the underlying principles that enable causal discovery.

4) We discuss how useful models of reality may be learned from data in the form of causal representations and discuss several current problems of machine learning from a causal point of view in Section VI.

5) We assay the implications of causality for practical machine learning in Section VII. Using causal language, we revisit robustness and generalization, as well as existing common practices, such as semi-supervised learning (SSL), self-supervised learning,
data augmentation, and pretraining. We discuss examples at the intersection between causality and machine learning in scientific applications and speculate on the advantages of combining the strengths of both fields to build a more versatile AI.

II. LEVELS OF CAUSAL MODELING
The gold standard for modeling natural phenomena is a set of coupled differential equations modeling physical mechanisms responsible for time evolution. This allows us to predict the future behavior of a physical system, reason about the effect of interventions, and predict statistical dependencies between variables that are generated by coupled time evolution. It also offers physical insights, explaining the functioning of the system, and lets us read off its causal structure. To this end, consider the coupled set of differential equations:

$$\frac{dx}{dt} = f(x), \quad x \in \mathbb{R}^d$$ (1)

with initial value $x(t_0) = x_0$. The Picard–Lindelöf theorem states that, at least locally, if $f$ is Lipschitz, there exists a unique solution $x(t)$. This implies, in particular, that the immediate future of $x$ is implied by its past values.

If we formally write this in terms of infinitesimal differentials $dt$ and $dx = x(t + dt) - x(t)$, we get

$$x(t + dt) = x(t) + dt \cdot f(x(t)).$$ (2)

From this, we can ascertain which entries of the vector $x(t)$ mathematically determine the future of others $x(t + dt)$. This tells us that if we have a physical system whose physical mechanisms are correctly described using such an ordinary differential equation (1), solved for $(dx/dt)$ (i.e., the derivative only appears on the left-hand side), then its causal structure can be directly read off.\(^2\)

While a differential equation is a rather comprehensive description of a system, a statistical model can be viewed as a much more superficial one. It often does not refer to dynamic processes; instead, it tells us how some of the variables allow the prediction of others as long as experimental conditions do not change. For example, if we drive a differential equation system with certain types of noise, or we average over time, then it may be the case that statistical dependencies between components of $x$ emerge and those can then be exploited by machine learning. Such a model does not allow us to predict the effect of interventions; however, its strength is that it can often be learned from observational data, while a differential equation usually requires an intelligent human to come up with it. Causal modeling lies in between these two extremes. Like models in physics, it aims to provide the understanding and predict the effect of interventions. However, causal discovery and learning try to arrive at such models in a data-driven way, replacing expert knowledge with weak and generic assumptions. The overall situation is summarized in Table 1, adapted from [188]. In the following, we address some of the tasks listed in Table 1 in more detail.

A. Predicting in the i.i.d. Setting
Statistical models are a superficial description of reality as they are only required to model associations. For a given set of input examples $X$ and target labels $Y$, we may be interested in approximating $P(Y|X)$ to answer questions, such as “what is the probability that this particular image contains a dog?” or “what is the probability of heart failure given certain diagnostic measurements (e.g., blood pressure) carried out on a patient?” Subject to suitable assumptions, these questions can be provably answered by observing a sufficiently large amount of i.i.d. data from $P(X, Y)$ [257]. Despite the impressive advances of machine learning, causality offers an underexplored complement: accurate predictions may not be sufficient to inform decision-making. For example, the frequency of storks is a reasonable predictor for human birth rates in Europe [168]. However, as there is no direct causal link between these two variables, a change to the stork population would not affect the birth rates, even though a statistical model may predict so. The predictions of a statistical model are only accurate within identical experimental

\(^2\)Note that this requires that the differential equation system describes the causal physical mechanisms. If, in contrast, we considered a set of differential equations that phenomenologically correctly describe the time evolution of a system without capturing the underlying mechanisms (e.g., due to unobserved confounding or a form of course graining that does not preserve the causal structure [208]), then (2) may not be causally meaningful [186], [217].
conditions. Performing an intervention changes the data distribution, which may lead to (arbitrarily) inaccurate predictions [183], [188], [220], [237].

B. Predicting Under Distribution Shifts

Interventional questions are more challenging than predictions as they involve actions that take us out of the usual i.i.d. setting of statistical learning. Interventions may affect both the value of a subset of causal variables and their relations. For example, “is increasing the number of storks in a country going to boost its human birth rate?” and “would fewer people smoke if cigarettes were more socially stigmatized?” As interventions change the joint distribution of the variables of interest, classical statistical learning guarantees [257] no longer apply. On the other hand, learning about interventions may allow training predictive models that are robust against the changes in distribution that naturally happen in the real world. Here, interventions do not need to be deliberate actions to achieve a goal. Statistical relations may change dynamically over time (e.g., people’s preferences and tastes), or there may simply be a mismatch between a carefully controlled training distribution and the test distribution of a model deployed in production. The robustness of deep neural networks has recently been scrutinized and become an active research topic related to causal inference. We argue that predicting under distribution shift should not be reduced to just the accuracy on a test set. If we wish to incorporate learning algorithms into human decision-making, we need to trust that the predictions of the algorithm will remain valid if the experimental conditions are changed.

C. Answering Counterfactual Questions

Counterfactual problems involve reasoning about why things happened, imagining the consequences of different actions in hindsight, and determining which actions would have achieved the desired outcome. Answering counterfactual questions can be more difficult than answering interventional questions. However, this may be a key challenge for AI, as an intelligent agent may benefit from imagining the consequences of its actions and understanding in retrospect what led to certain outcomes, at least to some degree of approximation.\(^3\) We have mentioned the example of statistical predictions of heart failure above. An interventional question would be “how does the probability of heart failure change if we convince a patient to exercise regularly?” A counterfactual one would be “would a given patient have suffered heart failure if they had started exercising a year earlier?” As we shall discuss in the following, counterfactuals, or approximations thereof, are especially critical in RL. They can enable agents to reflect on their decisions and formulate hypotheses that can be empirically verified in a process akin to the scientific method.

D. Nature of Data: Observational, Interventional, and (Un)structured

The data format plays a substantial role in which type of relation can be inferred. We can distinguish two axes of data modalities: observational versus interventional, and hand-engineered versus raw (unstructured) perceptual input.

1) Observational and Interventional Data: An extreme form of data which is often assumed but seldom strictly available is observational i.i.d. data, where each data point is independently sampled from the same distribution. Another extreme is interventional data with known interventions, where we observe data sets sampled from multiple distributions each of which is the result of a known intervention. In between, we have data with (domain) shifts or unknown interventions. This is observational in the sense that the data is only observed passively, but it is interventional in the sense that there are interventions/shifts, but unknown to us.

2) Hand-Engineered Data Versus Raw Data: Especially, in classical AI, data are often assumed to be structured into high level and semantically meaningful variables, which may partially (modulo some variables being unobserved) correspond to the causal variables of the underlying graph. Raw data, in contrast, are unstructured and do not expose any direct information about causality.

While statistical models are weaker than causal models, they can be efficiently learned from observational data alone on both hand-engineered features and raw perceptual input, such as images, videos, and speech. On the other hand, although methods for learning causal structure from observations exist [18], [37], [83], [113], [123], [139], [161], [174]–[176], [188]–[190], [229], [237], [246], [279], learning causal relations frequently requires collecting data from multiple environments or the ability to perform interventions [251]. In some cases, it is assumed that all common causes of measured variables are also observed (causal sufficiency).\(^4\) Overall, a significant amount of prior knowledge is encoded in which variables are measured. Moving forward, one would hope to develop methods that replace expert data collection with suitable inductive biases and learning paradigms, such as metalearning and self-supervision. If we wish to learn a causal model that is useful for a particular set of tasks and environments, the appropriate granularity of the high-level

\(^3\)Note that two types of questions occupy a continuum: to this end, consider a probability that is both conditional and interventional \(P(A|B, do(C))\). If \(B\) is an empty set, we have a classical intervention; if \(B\) contained all (unobserved) noise terms, we have a counterfactual. If \(B\) is not identical to the noise terms, but, nevertheless, informative about them, we get something in between. For instance, reinforcement learning (RL) practitioners may call \(Q\) functions as providing counterfactuals even though they model \(P\) [return from \(t\) agent state at time \(t\), do (action at time \(t\))] and, therefore, closer to an intervention (which is why they can be estimated from data).

\(^4\)There are also algorithms that do not require causal sufficiency [237].
variables depends on the tasks of interest and on the type of data that we have at our disposal, for example, which interventions can be performed and what is known about the domain.

III. CAUSAL MODELS AND INFERENCE

As discussed, reality can be modeled at different levels, from the physical one to statistical associations between epiphenomena. In this section, we expand on the difference between statistical and causal modeling and review a formal language to talk about interventions and distribution changes.

A. Methods Driven by i.i.d. Data

The machine learning community has produced impressive successes with machine learning applications to big data problems [54], [148], [171], [223], [232]. In these successes, there are several trends at work [215]: 1) we have massive amounts of data, often from simulations or large-scale human labeling; 2) we use high-capacity machine learning systems (i.e., complex function classes with many adjustable parameters); 3) we employ high-performance computing systems; and (often ignored, but crucial when it comes to causality) 4) the problems are i.i.d. The latter can be guaranteed by the construction of a task, including training and test set (e.g., image recognition using benchmark data sets). Alternatively, problems can be made approximately i.i.d., for example, by carefully collecting the right training set for a given application problem, or by methods, such as “experience replay” [171] where an RL agent stores observations in order to later permute them for the purpose of retraining.

For i.i.d. data, strong universal consistency results from statistical learning theory apply, guaranteeing convergence of a learning algorithm to the lowest achievable risk. Such algorithms do exist, for instance, nearest neighbor classifiers, support vector machines, and neural networks [67], [221], [239], [257]. Seen in this light, it is not surprising that we can indeed match or surpass human performance if given enough data. However, current machine learning methods often perform poorly when faced with problems that violate the i.i.d. assumption, yet seem trivial to humans. Vision systems can be grossly misled if an object that is normally recognized with high accuracy is placed in a context that in the training set may be negatively correlated with the presence of the object. Distribution shifts may also arise from simple corruptions that are common in real-world data collection pipelines [10], [107], [129], [170], [206]. An example of this is the impact of socioeconomic factors in clinics in Thailand on the accuracy of a detection system for diabetic retinopathy [19]. More dramatically, the phenomenon of “adversarial vulnerability” [249] highlights how even tiny but targeted violations of the i.i.d. assumption, generated by adding suitably chosen perturbations to images, imperceptible to humans, can lead to dangerous errors, such as confusion of traffic signs.

Overall, it is fair to say that much of the current practice (of solving i.i.d. benchmark problems) and most theoretical results (about generalization in i.i.d. settings) fail to tackle the hard open challenge of generalization across problems.

To further understand how the i.i.d. assumption is problematic, let us consider a shopping example. Suppose that Alice is looking for a laptop rucksack on the Internet (i.e., a rucksack with a padded compartment for a laptop). The web shop’s recommendation system suggests that she should buy a laptop to go along with the rucksack. This seems odd because she probably already has a laptop; otherwise, she would not be looking for the rucksack in the first place. In a way, the laptop is the cause, and the rucksack is an effect. Now, suppose that we are told whether a customer has bought a laptop. This reduces our uncertainty about whether she also bought a laptop rucksack, and vice versa—and it does so by the same amount (the mutual information), so the directionality of cause and effect is lost. However, the directionality is present in the physical mechanisms generating statistical dependence, for instance, the mechanism that makes a customer want to buy a rucksack once she owns a laptop. Recommending an item to buy constitutes an intervention in a system, taking us outside the i.i.d. setting. We no longer work with the observational distribution but a distribution where certain variables or mechanisms have changed.

B. Reichenbach Principle: From Statistics to Causality

Reichenbach [198] clearly articulated the connection between causality and statistical dependence. He postulated the following:

Common cause principle: If two observables $X$ and $Y$ are statistically dependent, then there exists a variable $Z$ that causally influences both and explains all the dependence in the sense of making them independent when conditioned on $Z$.

As a special case, this variable can coincide with $X$ or $Y$. Suppose that $X$ is the frequency of storks and $Y$ the human birth rate. If storks bring the babies, then the correct causal graph is $X \rightarrow Y$. If babies attract storks, it is $X \leftarrow Y$. If there is some other variable that causes both (such as economic development), we have $X \leftarrow Z \rightarrow Y$.

Without additional assumptions, we cannot distinguish these cases using observational data. The class of observational distributions over $X$ and $Y$ that can be realized by these models is the same in all three cases. A causal model, thus, contains genuinely more information than a statistical one.

While causal structure discovery is hard if we have only two observables [190], the case of more observables is surprisingly easier, the reason being that, in that case, there are nontrivial conditional independence properties [52].
[75], [238] implied by causal structure. These generalize the
Reichenbach principle and can be described by using
the language of causal graphs or structural causal mod-
els (SCMs), merging probabilistic graphical models and
the notion of interventions [183], [237]. They are best
described using directed functional parent–child relation-
ships rather than conditionals. While conceptually simple
in hindsight, this constituted a major step in the under-
standing of causality.

C. Structural Causal Models

The SCM viewpoint considers a set of observables (or
variables) $X_1, \ldots, X_n$ associated with the vertices of a
directed acyclic graph (DAG). We assume that each observ-
able is the result of an assignment

$$X_i := f_i(P\!A_i, U_i) \quad (i = 1, \ldots, n) \quad (3)$$

using a deterministic function $f_i$ depending on $X_i$’s parents
in the graph (denoted by $P\!A_i$) and on an unexplained
random variable $U_i$. Mathematically, the observables are,
thus, random variables, too. Directed edges in the graph
represent direct cause since the parents are connected to
$X_i$ by directed edges and, through (3), directly affect
the assignment of $X_i$. The noise $U_i$ ensures that the overall
object (3) can represent a general conditional distribution
$P(X_i \mid P\!A_i)$, and the set of noises $U_1, \ldots, U_n$ is assumed
to be jointly independent. If they were not, then, by the
common cause principle, there should be another variable
that causes their dependence, and thus, our model would
not be causally sufficient.

If we specify the distributions of $U_1, \ldots, U_n$, recursive
application of (3) allows us to compute the entangled obser-
vational joint distribution $P(X_1, \ldots, X_n)$. This distribution
has structural properties inherited from the graph [147],
[183]: it satisfies the causal Markov condition stating that
conditioned on its parents, each $X_j$ is independent of its
nondescendants.

Intuitively, we can think of the independent noises as
“information probes” that spread through the graph (much
like independent elements of gossip can spread through a
social network). Their information gets entangled, man-
ifesting itself in a footprint of conditional dependencies,
making it possible to infer aspects of the graph structure
from observational data using independence testing. Like
in the gossip analogy, the footprint may not be suffi-
ciently characteristic to pin down a unique causal struc-
ture. In particular, it certainly is not if there are only
two observables since any nontrivial conditional indepen-
dence statement requires at least three variables. The two-
variable problem can be addressed by making additional
assumptions, as not only the graph topology leaves a foot-
print in the observational distribution, but the functions
$f_i$ do, too. This point is interesting for machine learning,
where much attention is devoted to properties of function
classes (e.g., priors or capacity measures), and we shall
return to it below.

1) Causal Graphical Models: The graph structure along
with the joint independence of the noises implies a canonical
factorization of the joint distribution entailed by (3)
into causal conditionals that we refer to as the causal (or
disentangled) factorization

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid P\!A_i). \quad (4)$$

While many other entangled factorizations are possible, for
example,

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid X_{i+1}, \ldots, X_n) \quad (5)$$

the factorization (4) yields practical computational advan-
tages during inference, which is, in general, hard, even
when it comes to nontrivial approximations [210]. But
more interestingly, it is the only one that decomposes the
joint distribution into conditionals corresponding to the
structural assignments [see (3)]. We think of these as the
causal mechanisms that are responsible for all statistical
dependencies among the observables. Accordingly, in con-
trast to (5), the disentangled factorization represents the
joint distribution as a product of causal mechanisms.

2) Latent Variables and Confounders: Variables in a
causal graph may be unobserved, which can make causal
inference particularly challenging. Unobserved variables
may confound two observed variables so that they either
appear statistically related while not being causally related
(i.e., neither of the variables is an ancestor of the
other), or their statistical relation is altered by the presence
of the confounder (e.g., one variable is a causal ancestor
for the other, but the confounder is a causal ancestor of
both). Confounders may or may not be known or observed.

3) Interventions: The SCM language makes it straight-
forward to formalize interventions as operations that mod-
ify a subset of assignments (3), for example, changing $U_i$,
setting $f_i$ (and thus $X_i$) to a constant, or changing the
functional form of $f_i$ (and, thus, the dependence of $X_i$ on
its parents) [183], [237].

Several types of interventions may be possible [63],
which can be categorized as follows.

1) No intervention: Only observational data are obtained
from the causal model.

2) Hard/perfect: The function in the structural assign-
ment [see (3)] of a variable (or, analogously, of mul-
tiple variables) is set to a constant (implying that the
value of the variable is fixed), and then, the entailed
distribution for the modified SCM is computed.

3) Soft/imperfect: The structural assignment (3) for a
variable is modified by changing the function or the
noise term (this corresponds to changing the condi-
tional distribution given its parents).
4) Uncertain: The learner is not sure which mechanism/variable is affected by the intervention.

One could argue that stating the structural assignments as in (3) is not yet sufficient to formulate a causal model. In addition, one should specify the set of possible interventions on the SCM. This may be done implicitly via the functional form of structural equations by allowing any intervention over the domain of the mechanisms. This becomes relevant when learning a causal model from data, as the SCM depends on the interventions. Pragmatically, we should aim at learning causal models that are useful for specific sets of tasks of interest [208], [266] on appropriate descriptors (in terms of which causal statements they support) that must either be provided or learned. We will return to the assumptions that allow learning causal models and features in Section IV.

D. Difference Between Statistical Models, Causal Graphical Models, and SCMs

An example of the difference between a statistical and a causal model is depicted in Fig. 1. A statistical model may be defined, for instance, through a graphical model, that is, a probability distribution along with a graph such that the former is Markovian with respect to the latter [in which case it can be factorized as (4)]. However, the edges in a (generic) graphical model do not need to be causal [98]. For instance, the two graphs $X_1 \rightarrow X_2 \rightarrow X_3$ and $X_1 \leftarrow X_2 \leftarrow X_3$ imply the same conditional independence(s) ($X_1$ and $X_3$ are independent given $X_2$). They are, thus, in the same Markov equivalence class, that is, if a distribution is Markovian with respect to one of the graphs, then it also is with respect to the other graph. Note that the above serves as an example that the Markov condition is not sufficient for causal discovery. Further assumptions are needed (see below and [183], [188], and [237]).

A graphical model becomes causal if the edges of its graph are causal (in which case the graph is referred to as a “causal graph”) [see (3)]. This allows us to compute interventional distributions, as depicted in Fig. 1. When a variable is intervened upon, we disconnect it from its parents, fix its value, and perform ancestral sampling on its children.

An SCM is composed of: 1) a set of causal variables and 2) a set of structural equations with a distribution over the noise variables $U_i$ (or a set of causal conditionals). While both causal graphical models and SCMs allow computing interventional distributions, only the SCMs allow computing counterfactuals. To compute counterfactuals, we need to fix the value of the noise variables. Moreover, there are many ways to represent a conditional as a structural assignment (by picking different combinations of functions and noise variables).

Causal learning and reasoning: The conceptual basis of statistical learning is a joint distribution $P(X_1, \ldots, X_n)$ (where, often, one of the $X_i$ is a response variable denoted by $Y$), and we make assumptions about function classes used to approximate, say, a regression $E[Y | X]$. Causal learning considers a richer class of assumptions and seeks to exploit the fact that the joint distribution possesses a causal factorization [see (4)]. It involves the causal conditionals $P(X_i | \text{PA}_i)$ [e.g., represented by the functions $f_i$ and the distribution of $U_i$ in (3)], how these conditionals relate to each other, and interventions or changes that they admit. Once a causal model is available, either by external human knowledge or a learning process, causal reasoning allows drawing conclusions on the effect of interventions, counterfactuals, and potential outcomes. In contrast, statistical models only allow reasoning about the outcome of i.i.d. experiments.

IV. INDEPENDENT CAUSAL MECHANISMS

We now return to the disentangled factorization [see (4)] of the joint distribution $P(X_1, \ldots, X_n)$. This factorization according to the causal graph is always possible when $U_i$
Schölkopf et al.: Toward Causal Representation Learning

is independent, but we will now consider an additional notion of independence relating the factors in (4) to one another.

Whenever we perceive an object, our brain assumes that the object and the mechanism by which the information contained in its light reaches our brain are independent. We can violate this by looking at the object from an accidental viewpoint, which can give rise to optical illusions [188]. The above independence assumption is useful because, in practice, it holds most of the time, and our brain, thus, relies on objects being independent of our vantage point and the illumination. Likewise, there should not be accidental coincidences, such as 3-D structures lining up in 2-D, or shadow boundaries coinciding with texture boundaries. In vision research, this is called the generic viewpoint assumption.

If we move around the object, our vantage point changes, but we assume that the other variables of the overall generative process (e.g., lighting, object position, and structure) are unaffected by that. This is an invariance implied by the above independence, allowing us to infer 3-D information even without stereo vision (“structure from motion”).

For another example, consider a data set that consists of altitude $A$ and average annual temperature $T$ of weather stations [188]. $A$ and $T$ are correlated, which we believe is due to the fact that altitude has a causal effect on temperature. Suppose that we had two such data sets: one for Austria and one for Switzerland. The two joint distributions $P(A, T)$ may be rather different since the marginal distributions $P(A)$ over altitudes will differ. The conditionals $P(T|A)$, however, may be (close to) invariant since they characterize the physical mechanisms that generate temperature from altitude. This similarity is lost upon us if we only look at the overall joint distribution, without information about the causal structure $A \rightarrow T$.

The causal factorization $P(A)P(T|A)$ will contain a component $P(T|A)$ that generalizes across countries, while the entangled factorization $P(T)P(A|T)$ will exhibit no such robustness. Cum grano salis, the same applies when we consider interventions in a system. For a model to correctly predict the effect of interventions, it needs to be robust to generalizing from an observational distribution to certain interventional distributions.

One can express the above insights as follows [188], [220]:

\textit{ICM principle: The causal generative process of a system's variables is composed of autonomous modules that do not inform or influence each other. In the probabilistic case, this means that the conditional distribution of each variable given its causes (i.e., its mechanism) does not inform or influence the other mechanisms.}

This principle entails several notions important to causality, including separate intervenability of causal variables, modularity and autonomy of subsystems, and invariance [183], [188]. If we have only two variables, it reduces to independence between the cause distribution and the mechanism producing the effect distribution.

Applied to the causal factorization [see (4)], the principle tells us that the factors should be independent in the sense that the following holds.

1) Changing (or performing an intervention upon) one mechanism $P(X_i|PA_i)$ does not change any of the other mechanisms $P(X_j|PA_j)$ ($i \neq j$) [220].

2) Knowing some other mechanisms $P(X_i|PA_i)$ ($i \neq j$) does not give us information about a mechanism $P(X_j|PA_j)$ [124].

This notion of independence, thus, subsumes two aspects: the former pertaining to influence and the latter to invariance.

The notion of invariant, autonomous, and independent mechanisms has appeared in various guises throughout the history of causality research [72], [100], [111], [124], [183], [188], [240]. Early work on this was done by Haavelmo [100], stating the assumption that changing one of the structural assignments leaves the other ones invariant. Hoover [111] attributed to Herb Simon the invariance criterion: the true causal order is the one that is invariant under the right sort of intervention. Aldrich [4] discussed the historical development of these ideas in economics. He argued that the “most basic question one can ask about a relation should be: how autonomous is it?” [72, preface].

Pearl [183] discussed autonomy in detail, arguing that a causal mechanism remains invariant when other mechanisms are subjected to external influences. He pointed out that causal discovery methods may best work “in longitudinal studies conducted under slightly varying conditions, where accidental independencies are destroyed and only structural independencies are preserved.” Overviews are provided by Aldrich [4], Hoover [111], Pearl [183], and Peters et al. [188, Section 2.2]. These seemingly different notions can be unified [124], [240].

We view any real-world distribution as a product of causal mechanisms. A change in such a distribution (e.g., when moving from one setting/domain to a related one) will always be due to changes in at least one of those mechanisms. Consistent with the implication 1) of the ICM Principle, we state the following hypothesis:

\textit{Small distribution changes tend to manifest themselves in a sparse or local way in the causal/disentangled factorization [see (4)], that is, they should usually not affect all factors simultaneously.}

In contrast, if we consider a noncausal factorization, for example, (5), then many, if not all, terms will be affected simultaneously as we change one of the physical mechanisms responsible for a system’s statistical dependencies.

Such a factorization may, thus, be called entangled, a term that has gained popularity in machine learning [24], [110], [158], [247].
The SMS hypothesis was stated in [25], [114], [180], and [217] and in earlier form in [219], [220], and [281]. An intellectual ancestor is Simon’s invariance criterion, that is, that the causal structure remains invariant across changing background conditions [235]. The hypothesis is also related to ideas of looking for features that vary slowly [70], [270]. It has recently been used for learning causal models [131], modular architectures [29], [85], and disentangled representations [159].

We have informally talked about the dependence of two mechanisms $P(X_i | PA_i)$ and $P(X_j | PA_j)$ when discussing the ICM principle and the disentangled factorization [see (4)]. Note that the dependence of two such mechanisms does not coincide with the statistical dependence of the random variables $X_i$ and $X_j$. Indeed, in a causal graph, many of the random variables will be dependent even if all mechanisms are independent. Also, the independence of the noise terms $U_i$ does not translate into the independence of the $X_i$. Intuitively speaking, the independent noise terms $U_i$ provide and parameterize the uncertainty contained in the fact that a mechanism $P_i(X_i | PA_i)$ is nondeterministic and, thus, ensure that each mechanism adds an independent element of uncertainty. In this sense, the ICM principle contains the independence of the unexplained noise terms in an SCM [see (3)] as a special case.

In the ICM principle, we have stated that independence of two mechanisms (formalized as conditional distributions) should mean that the two conditional distributions do not inform or influence each other. The latter can be thought of as requiring that independent interventions are possible. To better understand the former, we next discuss a formalization in terms of algorithmic independence. In a nutshell, we encode each mechanism as a bit string and require that joint compression of these strings does not save space relative to independent compressions.

To this end, first recall that we have, so far, discussed links between causal and statistical structures. Of the two, the more fundamental one is the causal structure since it captures the physical mechanisms that generate statistical dependencies in the first place. The statistical structure is an epiphenomenon that follows if we make the unexplained variables random. It is awkward to talk about statistical information contained in a mechanism since deterministic functions in the generic case neither generate nor destroy information. This serves as a motivation to devise an alternative model of causal structures in terms of the Kolmogorov complexity [124]. The Kolmogorov complexity (or algorithmic information) of a bit string is essentially the length of its shortest compression on a Turing machine and, thus, a measure of its information content. Independence of mechanisms can be defined as vanishing mutual algorithmic information, that is, two conditionals are considered independent if knowing (the shortest compression of) one does not help us achieve a shorter compression of the other.

The algorithmic information theory provides a natural framework for nonstatistical graphical models [120], [124]. Just like the latter is obtained from SCMs by making the unexplained variables $U_i$ random, we obtain algorithmic graphical models by making the $U_i$ bit strings, jointly independent across nodes, and viewing $X_i$ as the output of a fixed Turing machine running the program $U_i$ on the input $PA_i$. Similar to the statistical case, one can define a local causal Markov condition, a global one in terms of $d$-separation, and an additive decomposition of the joint Kolmogorov complexity in analogy to (4), and prove that they are implied by the SCM [124]. Interestingly, in this case, independence of noises and independence of mechanisms coincide since the independent programs play the role of the unexplained noise terms. This approach shows that causality is not intrinsically bound to statistics.

V. CAUSAL DISCOVERY AND MACHINE LEARNING

Let us turn to the problem of causal discovery from data. Subject to suitable assumptions, such as faithfulness [237], one can sometimes recover aspects of the underlying graph from observational data by performing conditional independence tests. However, there are several problems with this approach. One is that our data sets are always finite in practice, and conditional independence testing is a notoriously difficult problem, especially if conditioning sets are continuous and multidimensional. Thus, while, in principle, the conditional independencies implied by the causal Markov condition hold irrespective of the complexity of the functions appearing in an SCM, for finite data sets, conditional independence testing is hard without additional assumptions [225]. Recent progress in (conditional) independence testing heavily relies on kernel function classes to represent probability distributions in reproducing kernel Hilbert spaces [43], [61], [74], [91], [92], [193], [280]. The other problem is that, in the case of only two variables, the ternary concept of conditional independence collapses and the Markov condition, thus, has no nontrivial implications.

It turns out that both problems can be addressed by making assumptions on function classes. This is typical for machine learning, where it is well known that finite-sample generalization without assumptions on function classes is impossible. Specifically, although there are universally consistent learning algorithms, that is, approaching minimal expected error in the infinite sample limit, there are always cases where this convergence is arbitrarily slow. Thus, for given sample size, it will depend on the problem being learned whether we achieve low expected error, and the statistical learning theory provides probabilistic guarantees.

---

6In the sense that the mapping from $PA_i$ to $X_i$ is described by a nontrivial conditional distribution, rather than by a function.

7One can recover the causal structure up to a Markov equivalence class, where DAGs have the same undirected skeleton and “immoralities” ($X_i \rightarrow X_j \leftarrow X_k$).
in terms of measures of complexity of function classes [56], [257].

Returning to causality, we provide an intuition why assumptions on the functions in an SCM should be necessary to learn about them from data. Consider a toy SCM with only two observables $X \rightarrow Y$. In this case, (3) turns into

$$X = U$$
$$Y = f(X, V)$$

with $U \perp \perp V$. Now, think of $V$ acting as a random selector variable choosing from among a set of functions $\mathcal{F} = \{f_v(x) \equiv f(x, v) \mid v \in \text{supp}(V)\}$. If $f(x, v)$ depends on $v$ in a nonsmooth way, it should be hard to glean information about the SCM from a finite data set, given that $V$ is not observed and its value randomly selects among arbitrarily different $f_v$.

This motivates restricting the complexity with which $f$ depends on $V$. A natural restriction is to assume an additive noise model

$$X = U$$
$$Y = f(X) + V.$$}

If $f$ in (7) depends smoothly on $V$, and if $V$ is relatively well concentrated, this can be motivated by a local Taylor expansion argument. It drastically reduces the effective size of the function class—without such assumptions, the latter could depend exponentially on the cardinality of the support of $V$. Restrictions of function classes not only make it easier to learn functions from data but it turns out that they can break the symmetry between cause and effect in the two-variable case: one can show that, given a distribution over $X, Y$ generated by an additive noise model, one cannot fit an additive noise model in the opposite direction (i.e., with the roles of $X$ and $Y$ interchanged) [18], [113], [139], [175], [190] (see also [246]). This is subject to certain genericity assumptions, and notable exceptions include the case where $U$ and $V$ are Gaussian and $f$ is linear. It generalizes results of Shimizu et al. [229] for linear functions, and it can be generalized to include nonlinear rescalings [279], loops [174], confounders [123], and multivariable settings [189].

Empirically, there is a number of methods that can detect causal direction better than chance [176], some of the building on the above Kolmogorov complexity model [37], some on generative models [83], and some directly learning to classify bivariate distributions into causal versus anticausal [161].

While restrictions of function classes are one possibility to allow identifying the causal structure, other assumptions or scenarios are possible. So far, we have discussed that causal models are expected to generalize under certain distribution shifts since they explicitly model interventions. By the SMS hypothesis, much of the causal structure is assumed to remain invariant. Hence, distribution shifts, such as observing a system in different “environments/contexts,” can significantly help to identify causal structure [188], [251]. These contexts can come from interventions [187], [191], [220], nonstationary time series [101], [116], [192], or multiple views [90], [114]. The contexts can likewise be interpreted as different tasks, which provides a connection to metalearning [23], [68], [213].

The work of Bengio et al. [25] ties the generalization in metalearning to invariance properties of causal models, using the idea that a causal model should adapt faster to interventions than purely predictive models. This was extended to multiple variables and unknown interventions in [131], proposing a framework for causal discovery using neural networks by turning the discrete graph search into a continuous optimization problem. While Bengio et al. [25] and Ke et al. [131] focused on learning a causal model using neural networks with an unsupervised loss, the work of Dasgupta et al. [51] explores learning a causal model using an RL agent. These approaches have in common that semantically meaningful abstract representations are given and do not need to be learned from high-dimensional and low-level (e.g., pixel) data.

VI. LEARNING CAUSAL VARIABLES

Traditional causal discovery and reasoning assume that the units are random variables connected by a causal graph. However, real-world observations are usually not structured into those units, to begin with, for example, objects in images [162]. Hence, the emerging field of causal representation learning strives to learn these variables from data, much like machine learning went beyond symbolic AI not requiring that the symbols that algorithms manipulate be given a priori (see [34]). To this end, we could try to connect causal variables $S_1, \ldots, S_n$ to observations

$$X = G(S_1, \ldots, S_n)$$

where $G$ is a nonlinear function. An example can be seen in Fig. 2, where high-dimensional observations are the result of a view on the state of a causal system that is then processed by a neural network to extract high-level variables that are useful on a variety of tasks. Although causal models in economics, medicine, or psychology often use variables that are abstractions of underlying quantities, it is challenging to state general conditions under which coarse-grained variables admit causal models with well-defined interventions [42], [208]. Defining objects or variables that can be causally related amounts to coarse-graining of more detailed models of the world, including microscopic structural equation models [208], ordinary differential equations [173], [207], and temporally aggregated time series [79]. The task of identifying suitable units that admit causal models is challenging for both human and machine intelligence. Still, it aligns with
Fig. 2. Illustration of the causal representation learning problem setting. Perceptual data, such as images or other high-dimensional sensor measurements, can be thought of as entangled views of the state of an unknown causal system, as described in (10). With the exception of possible task labels, none of the variables describing the causal variables generating the system may be known. The goal of causal representation learning is to learn a representation (partially) exposing this unknown causal structure (e.g., which variables describe the system, and their relations). As full recovery may often be unreasonable, neural networks may map the low-level features to some high-level variables supporting causal statements relevant to a set of downstream tasks of interest. For example, if the task is to detect the manipulable objects in a scene, the representation may separate intrinsic object properties from their pose and appearance to achieve robustness to distribution shifts on the latter variables. Usually, we do not get labels for the high-level variables, but the properties of causal models can serve as useful inductive biases for learning (e.g., the SMS hypothesis).

Fig. 3. Example of the SMS hypothesis where an intervention (which may or may not be intentional/observed) changes the position of one finger (X), and as a consequence, the object falls. The change in pixel space is entangled (or distributed), in contrast to the change in the causal model.

Thus, the feasibility of the disentangled representation

\[
P(S_1, \ldots, S_n) = \prod_{i=1}^{n} P(S_i \mid PA_i) \tag{11}
\]

as well as the property that the conditionals \(P(S_i \mid PA_i)\) are independently manipulable and largely invariant across related problems. Suppose that we seek to reconstruct such a disentangled representation using independent mechanisms [see (11)] from data, but the causal variables \(S\) are not provided to us \textit{a priori}. Rather, we are given (possibly high-dimensional) \(X = (X_1, \ldots, X_d)\) (in the following, we think of \(X\) as an image with pixels \(X_1, \ldots, X_d\), as in (10), from

A. Problem 1—Learning Disentangled Representations

We have earlier discussed the ICM principle implying both the independence of the SCM noise terms in (3) and, the general goal of modern machine learning to learn meaningful representations of data, where meaningful can include robust, explainable, or fair [130], [134], [142], [259], [275].

To combine structural causal modeling [see (3)] and representation learning, we should strive to embed an SCM into larger machine learning models whose inputs and outputs may be high-dimensional and unstructured, but whose inner workings are at least partly governed by an SCM (that can be parameterized with a neural network). The result may be a modular architecture, where the different modules can be individually fine-tuned and repurposed for new tasks [85], [180], and the SMS hypothesis can be used to enforce the appropriate structure. We visualize an example in Fig. 3 where changes are sparse for the appropriate causal variables (the position of the finger and the cube changed as a result of moving the finger) but dense in other representations, for example, in the pixel space (as finger and cube move, many pixels change their value). At the extreme, all pixels may change as a result of a sparse intervention, for example, if the camera view or the lighting changes.

We now discuss three problems of modern machine learning in the light of causal representation learning.
which we should construct causal variables \( S_1, \ldots, S_n \) \((n \ll d)\) as well as mechanisms [see (3)]

\[
S_i := f_i({\mathbf{PA}_i, U_i}) \quad (i = 1, \ldots, n) \tag{12}
\]

modeling the causal relationships among \( S_i \). To this end, as a first step, we can use an encoder \( q : \mathbb{R}^d \rightarrow \mathbb{R}^n \) taking \( X \) to a latent “bottleneck” representation comprising the unexplained noise variables \( U = (U_1, \ldots, U_n) \). The next step is the mapping \( f(U) \) determined by the structural assignments \( f_1, \ldots, f_n \). Finally, we apply a decoder \( p : \mathbb{R}^n \rightarrow \mathbb{R}^d \). For suitable \( n \), the system can be trained using reconstruction error to satisfy \( p \circ f \circ q \approx id \) on the observed images. If the causal graph is known, the topology of a neural network implementing \( f \) can be fixed accordingly; if not, the neural network decoder learns the composition \( \tilde{p} = p \circ f \). In practice, one may not know \( f \) and, thus, only learn an autoencoder \( \tilde{p} \circ q \), where the causal graph effectively becomes an unspecified part of the decoder \( \tilde{p} \), possibly aided by a suitable choice of architecture [149].

Much of the existing work on disentanglement [62], [110], [135], [157]–[159], [202], [256] focuses on independent factors of variation. This can be viewed as the special case where the causal graph is trivial, that is, \( \forall i : \mathbf{PA}_i = \emptyset \) in (12). In this case, the factors are functions of the independent exogenous noise variables and, thus, independent themselves.\(^8\) However, the ICM principle is more general and contains statistical independence as a special case.

Note that the problem of object-centric representation learning [11], [40], [84], [87], [88], [138], [155], [160], [255], [262] can also be considered a special case of disentangled factorization as discussed here. Objects are constituents of scenes that in principle permit separate interventions. A disentangled representation of a scene containing objects should probably use objects as some of the building blocks of an overall causal factorization,\(^9\) complemented by mechanisms, such as orientation, viewing direction, and lighting.

The problem of recovering the exogenous noise variables is ill-defined in the i.i.d. case as there are infinitely many equivalent solutions yielding the same observational distribution [117], [158], [188]. Additional assumptions or biases can help favoring certain solutions over others [158], [205]. Leeb et al. [149] propose a structured decoder that embeds an SCM and automatically learns a hierarchy of disentangled factors.

To make (12) causal, we can use the ICM principle, that is, we should make \( U_i \) statistically independent, and we should make the mechanisms independent. This could be done by ensuring that they are invariant across problems, exhibit sparse changes to actions or that they can be independently intervened upon [22], [30], [217]. Locatello et al. [159] showed that the SMS hypothesis stated above is theoretically sufficient when given suitable training data. Furthermore, the SMS hypothesis can be used as supervision signal, in practice, even if \( \mathbf{PA}_i \neq \emptyset \) [252]. However, which factors of variation can be disentangled depend on which interventions can be observed [159], [230]. As discussed by Schölkopf et al. [219] and Shu et al. [230], different supervision signals may be used to identify subsets of factors. Similarly, when learning causal variables from data, which variables can be extracted and their granularity depends on which distribution shifts, explicit interventions, and other supervision signals are available.

B. Problem 2—Learning Transferable Mechanisms

An artificial or natural agent in a complex world is faced with limited resources. This concerns training data, that is, we only have limited data for each task/domain, and, thus, need to find ways of pooling/reusing data, in stark contrast to the current industry practice of large-scale labeling work done by humans. It also concerns computational resources: animals have constraints on the size of their brains, and evolutionary neuroscience knows many examples where brain regions get repurposed. Similar constraints on size and energy apply as ML methods get embedded in (small) physical devices that may be battery-powered. Future AI models that robustly solve a range of problems in the real world will, thus, likely need to reuse components, which requires them to be robust across tasks and environments [219]. An elegant way to do this is to employ a modular structure that mirrors corresponding modularity in the world. In other words, if the world is indeed modular, in the sense that components/mechanisms of the world play roles across a range of environments, tasks, and settings, then it would be prudent for a model to employ corresponding modules [85]. For instance, if variations of natural lighting (the position of the sun, clouds, and so on) imply that the visual environment can appear in brightness conditions spanning several orders of magnitude, then visual processing algorithms in our nervous system should employ methods that can factor out these variations, rather than building separate sets of face recognizers, say, for every lighting condition. If, for example, our nervous system were to compensate for the lighting changes by a gain control mechanism, then this mechanism in itself need not have anything to do with the physical mechanisms bringing about brightness differences. However, it would play a role in a modular structure that corresponds to the role that the physical mechanisms play in the world’s modular structure. This could produce a bias toward models that exhibit certain forms of structural homomorphism to a world that we cannot directly recognize, which would be rather intriguing, given that ultimately our brains do nothing but turn neuronal signals into other neuronal
signals. A sensible inductive bias to learn such models is to look for ICMs [182], and competitive training can play a role in this. For pattern recognition tasks, Parascandolo et al. [180] and Goyal et al. [85] suggested that learning causal models that contain independent mechanisms may help in transferring modules across substantially different domains.

C. Problem 3—Learning Interventional World Models and Reasoning

Deep learning excels at learning representations of data that preserve relevant statistical properties [24], [148]. However, it does so without taking into account the causal properties of the variables, that is, it does not care about the interventional properties of the variables that it analyzes or reconstructs. Causal representation learning should move beyond the representation of statistical dependence structures toward models that support intervention, planning, and reasoning, realizing Konrad Lorenz’ notion of thinking as acting in an imagined space [163]. This ultimately requires the ability to reflect back on one’s actions and envision alternative scenarios, possibly necessitating (the illusion of) free will [184]. The biological function of self-consciousness may be related to the mental function of self-consciousness may be related to the imaging space, and free will may then be a means to communicate about actions taken by that variable, crucial for social and cultural learning, a topic that has not yet entered the stage of machine learning research although it is at the core of human intelligence [108].

VII. IMPLICATIONS FOR MACHINE LEARNING

All these discussions call for a learning paradigm that does not rest on the usual i.i.d. assumption. Instead, we wish to make a weaker assumption that the data on which the model will be applied comes from a possibly different distribution but involving (mostly) the same causal mechanisms [188]. This raises serious challenges: 1) in many cases, we need to infer abstract causal variables from the available low-level input features; 2) there is no consensus on which aspects of the data reveal causal relations; 3) the usual experimental protocol of training and test set may not be sufficient for inferring and evaluating causal relations on existing data sets, and we may need to create new benchmarks, for example, with access to environmental information and interventions; 4) even in the limited cases that we understand, we often lack scalable and numerically sound algorithms. Despite these challenges, we argue that this endeavor has concrete implications for machine learning and may shed light on desiderata and current practices alike.

A. Semisupervised Learning

Suppose that our underlying causal graph is $X \rightarrow Y$, and at the same time, we are trying to learn a mapping $P(X, Y) = P(X)P(Y|X)$. The causal factorization (4) for this case is

$$P(X, Y) = P(X)P(Y|X).$$ (13)

The ICM principle posits that the modules in a joint distribution’s causal decomposition do not inform or influence each other. This means that, in particular, $P(X)$ should contain no information about $P(Y|X)$, which implies that SSL should be futile, in as far as it is using additional information about $P(X)$ (from unlabelled data) to improve our estimate of $P(Y|X = x)$.

In the opposite (anticausal) direction (i.e., the direction of prediction is opposite to the causal generative process), however, SSL may be possible. To see this, we refer to Daniušis et al. [50] who define a measure of dependence between input $P(X)$ and conditional $P(Y|X)$. Assuming that this measure is zero in the causal direction (applying the ICM assumption described in Section IV to the two-variable case), they show that it is strictly positive in the anticausal direction. Applied to SSL in the anticausal direction, this implies that the distribution of the input (now: effect) variable should contain information about the conditional output (cause) given input, that is, the quantity that machine learning is usually concerned with.

The study [220] empirically corroborated these predictions, thus establishing an intriguing bridge between the structure of learning problems and certain physical properties (cause–effect direction) of real-world data generating processes. It also led to a range of follow-up work [32], [78], [97], [114], [115], [152], [153], [156], [167], [195], [204], [243], [263], [267], [277], [278], [281], complementing the studies of Bareinboim and Pearl [14], [185], and it inspired a thread of work in the statistics community exploiting invariance for causal discovery and other tasks [105], [106], [114], [187], [191].

On the SSL side, subsequent developments include further theoretical analyses [125], [188, Section 5.1.2] and a form of conditional SSL [261]. The view of SSL as exploiting dependencies between a marginal $P(X)$ and a noncausal conditional $P(Y|X)$ is consistent with the common assumptions employed to justify SSL [45]. The cluster assumption asserts that the labeling function (which is a property of $P(Y|X)$) should not change within clusters of $P(X)$. The low-density separation assumption posits that the area where $P(Y|X)$ takes the value of 0.5 should have small $P(X)$; the semisupervised smoothness assumption, applicable also to continuous outputs, states that if two points in a high-density region are close and so should be the corresponding output values. Note, moreover, that some of the theoretical results in the field use assumptions well-known from causal graphs (even if they do not mention causality): the cotraining theorem [33] makes a statement about learnability from unlabelled data and

\[\text{10}\]Other dependence measures have been proposed for high-dimensional linear settings and time series [28], [119], [121], [122], [126], [226].
relies on an assumption of predictors being conditionally independent given the label, which we would normally expect if the predictors are (only) caused by the label, that is, an anticausal setting. This is nicely consistent with the above findings.

B. Adversarial Vulnerability

One can hypothesize that the causal direction should also have an influence on whether classifiers are vulnerable to adversarial attacks. These attacks have recently become popular and consist of minute changes to inputs, invisible to a human observer yet changing a classifier’s output [249]. This is related to causality in several ways. First, these attacks clearly constitute violations of the i.i.d. assumption that underlies statistical machine learning. If all we want to do is a prediction in an i.i.d. setting, then statistical learning is fine. In the adversarial setting, however, the modified test examples are not drawn from the same distribution as the training examples. The adversarial phenomenon also shows that the kind of robustness current classifiers exhibit is rather different from the one a human exhibits. If we knew both robustness measures, we could try to maximize one, while minimizing the other. Current methods can be viewed as crude approximations to this, effectively modeling the human’s robustness as a mathematically simple set, say, an $l_p$ ball of radius $\epsilon > 0$: they, often, try to find examples that lead to maximal changes in the classifier’s output, subject to the constraint that they lie in an $l_p$ ball in the pixel metric. As we think of a classifier as the approximation of a function, the large gradients exploited by these attacks are either property of this function or a defect of the approximation.

There are different ways of relating this to causal models. As described in [188, Section 1.4], different causal models can generate the same statistical pattern recognition model. In one of those, we might provide a writer with a sequence of class labels $y$, with the instruction to produce a set of corresponding images $x$. It is clear that intervening on $y$ will impact $x$, but intervening on $x$ will not impact $y$, so this is an anticausal learning problem. In another setting, we might ask the writer to decide for herself which digits to write and to record the labels alongside the digit (in this case, the classifier would try to predict one effect from another one, a situation that we might call a confounded one). In the last one, we might provide images to a person and ask the person to generate labels by classifying them.

Let us now assume that we are in the causal setting where the causal generative model factorizes into independent components, one of which is (essentially) the classification function. As discussed in Section III, when specifying a causal model, one needs to determine which interventions are allowed, and a structural assignment will then, by definition, be valid under every possible (allowed) intervention. One may, thus, expect that if the predictor approximates the causal mechanism that is inherently transferable and robust, adversarial examples should be harder to find [133], [216]. Recent work supports this view: it was shown that a possible defense against adversarial attacks is to solve the anticausal classification problem by modeling the causal generative direction, a method that, in vision, is referred to as analysis by synthesis [222]. A related defense method proceeds by reconstructing the input using an autoencoder before feeding it to a classifier [96].

C. Robustness and Strong Generalization

We can speculate that structures composed of autonomous modules, such as given by a causal factorization [see (4)], should be relatively robust to swapping out or modifying individual components. Robustness should also play a role when studying strategic behavior, that is, decisions or actions that take into account the actions of other agents (including AI agents). Consider a system that tries to predict the probability of successfully paying back a credit, based on a set of features. The set could include, for instance, the current debt of a person, as well as their address. To get a higher credit score, people could, thus, change their current debt (by paying it off), or they could change their address by moving to a more affluent neighborhood. The former probably has a positive causal impact on the probability of paying back; for the latter, this is less likely. Thus, we could build a scoring system that is more robust with respect to such strategic behavior by only using causal features as inputs [132].

To formalize this general intuition, one can consider a form of out-of-distribution generalization, which can be optimized by minimizing the empirical risk over a class of distributions induced by a causal model of the data [5], [169], [187], [204], [220]. To describe this notion, we start by recalling the usual empirical risk minimization setup. We have access to data from a distribution $P(X,Y)$ and train a predictor $g$ in a hypothesis space $\mathcal{H}$ (e.g., a neural network with a certain architecture predicting $Y$ from $X$) to minimize the empirical risk $\hat{R}$:

$$g^* = \arg \min_{g \in \mathcal{H}} \hat{R}_{P(X,Y)}(g)$$

where

$$\hat{R}_{P(X,Y)}(g) = \hat{E}_{P(X,Y)}[\text{loss}(Y,g(X))].$$

Here, we denote by $\hat{E}_{P(X,Y)}$ the empirical mean computed from a sample drawn from $P(X,Y)$. When we refer to “out-of-distribution generalization,” we mean having a small expected risk for a different distribution $P^!(X,Y)$:

$$R^\text{OOD}_{P^!(X,Y)}(g) = \mathbb{E}_{P^!(X,Y)}[\text{loss}(Y,g(X))].$$

$^{11}$Adversarial attacks may still exploit the quality of the (parameterized) approximation of a structural equation.
It is clear that the gap between \( \hat{R}_{P(X,Y)}(g) \) and \( R^{OOD}_{P^{i}(X,Y)}(g) \) will depend on how different the test distribution \( P^{i} \) is from the training distribution \( P \). To quantify this difference, we call environments the collection of different circumstances that give rise to the distribution shifts, such as locations, times, and experimental conditions. Environments can be modeled in a causal factorization [see (4)] as they can be seen as interventions on one or several causal variables or mechanisms. As a motivating example, one environment may correspond to where a measurement is taken (e.g., a certain room), and from each environment, we obtain a collection of measurements (images of objects in the same room). It is nontrivial (and, in some cases, provably hard [21]) to learn statistical models that are stable across training environments and generalize to novel testing environments [2], [5], [167], [187], [204] drawn from the same environment distribution.

Using causal language, one could restrict \( P^{i}(X,Y) \) to be the result of a certain set of interventions, that is, \( P^{i}(X,Y) \in \mathbb{P}_{G_{i}} \), where \( \mathbb{P}_{G_{i}} \) is a set of interventional distributions over a causal graph \( G_{i} \). The worst case out-of-distribution risk then becomes

\[
R^{OOD}_{\mathbb{P}_{G}}(g) = \max_{P^{i} \in \mathbb{P}_{G}} \mathbb{E}_{P^{i}(X,Y)} [\text{loss}(Y, g(X))]. \tag{17}
\]

To learn a robust predictor, we should have available a subset of environment distributions \( \mathcal{E} \subset \mathbb{P}_{G} \) and solve

\[
g^{*} = \underset{g \in \mathcal{H}}{\arg \min} \max_{P^{i} \in \mathcal{E}} \mathbb{E}_{P^{i}(X,Y)} [\text{loss}(Y, g(X))]. \tag{18}
\]

In practice, solving (18) requires specifying a causal model with an associated set of interventions. If the set of observed environments \( \mathcal{E} \) does not coincide with the set of possible environments \( \mathbb{P}_{G} \), we have an additional estimation error that may be arbitrarily large in the worst case [5], [21].

D. Pretraining, Data Augmentation, and Self-Supervision

Learning predictive models solving the min–max optimization problem of (18) is challenging. We now interpret several common techniques in machine learning as means of approximating (18).

The first approach is enriching the distribution of the training set. This does not mean obtaining more examples from \( P(X,Y) \) but training on a richer data set [54], [245], for example, through pretraining on a huge and diverse corpus [36], [46], [55], [60], [112], [137], [196], [253]. Since this strategy is based on standard empirical risk minimization, it can achieve stronger generalization in practice only if the new training distribution is sufficiently diverse to contain information about other distributions in \( \mathbb{P}_{G} \).

The second approach, often coupled with the previous one, is to rely on data augmentation to increase the diversity of the data by “augmenting” it through a certain type of artificially generated interventions [10], [140], [234]. For the visual domain, common augmentations include performing transformations, such as rotating the image, translating the image by a few pixels, or flipping the image horizontally. The high-level idea behind data augmentation is to encourage a system to learn underlying invariances or symmetries present in the augmented data distribution. For example, in a classification task, translating the image by a few pixels does not change the class label. One may view it as specifying a set of interventions \( \mathcal{E} \) that the model should be robust to (e.g., random crops/interpolations/translation/rotations). Instead of computing the maximum over all distributions in \( \mathcal{E} \), one can relax the problem by sampling from the interventional distributions and optimize an expectation over the different augmented images on a suitably chosen subset [39], using a search algorithm, such as RL [49] or an algorithm based on density matching [154].

The third approach is to rely on self-supervision to learn about \( P(X) \). Certain pretraining methods [36], [46], [55], [112], [196], [253] have shown that it is possible to achieve good results using only very few class labels by first pretraining on a large unlabeled data set and then fine-tuning on few labeled examples. Similarly, pretraining on large unlabeled image data sets can improve performance by learning representations that can efficiently transfer to a downstream task, as demonstrated by Bachman et al. [8], Chen et al. [47], Grill et al. [93], He et al. [102], and Oord et al. [179]. These methods fall under the umbrella of self-supervised learning, a family of techniques for converting an unsupervised learning problem into a supervised one by using the so-called pretext tasks with artificially generated labels without human annotations. The basic idea behind using pretext tasks is to force the learner to learn representations that contain information about \( P(X) \) that may be useful for (an unknown) downstream task. Much of the work on methods that use self-supervision relies on carefully constructing pretext tasks. A central challenge here is to extract features that are indeed informative about the data-generating distribution. Ideas from the ICM principle could help develop methods that can automate the process of constructing pretext tasks. Finally, one can explicitly optimize (18), for example, through adversarial training [80]. In that case, \( \mathbb{P}_{G} \) would contain a set of attacks that an adversary might perform, while, presently, we consider a set of natural interventions.

An interesting research direction is the combination of all these techniques, large-scale training, data augmentation, self-supervision, and robust fine-tuning on the available data from multiple, potentially simulated environments.

E. Reinforcement Learning

RL is closer to causality research than the machine learning mainstream in which it sometimes effectively
directly estimates do-probabilities. For example, on-policy learning estimates do-probabilities for the interventions specified by the policy (note that these may not be hard interventions if the policy depends on other variables). However, as soon as off-policy learning is considered, in particular, in the batch (or observational) setting [146], issues of causality become subtle [82], [165]. An emerging line of work devoted to the intersection of RL and causality includes [1], [13], [22], [38], [51], [165], [276]. Causal learning applied to RL can be divided into two aspects: causal induction and causal inference. Causal induction (discovery) involves learning causal relations from data, for example, an RL agent learning a causal model of the environment. Causal inference learns to plan and act based on a causal model. Causal induction in an RL setting poses different challenges than the classic causal learning settings where the causal variables are often given. However, there is accumulating evidence supporting the usefulness of an appropriate structured representation of the environment [2], [27], [258].

1) World Models: Model-based RL [68], [248] is related to causality as it aims at modeling the effect of actions (interventions) on the current state of the world. Particularly relevant for causal leaning are generative world models that capture some of the causal relations underlying the environment and serve as Lorenzian imagined spaces (see INTRODUCTION above) to train RL agents [48], [99], [127], [178], [214], [231], [248], [268], [271]. Structured generative approaches further aim at decomposing an environment into multiple entities with causally correct relations among them, modulo the completeness of the variables, and confounding [15], [44], [59], [136], [264], [265]. However, many of the current approaches (regardless of structure), only build partial models of the environment [89]. Since they do not observe the environment at every time step, the environment may become an unobserved confounder affecting both the agent’s actions and the reward. To address this issue, a model can use the backdoor criterion conditioning on its policy [200].

2) Generalization, Robustness, and Fast Transfer: While RL has already achieved impressive results, the sample complexity required to achieve consistently good performance is often prohibitively high. Furthermore, RL agents are often brittle (if data is limited) in the face of even tiny changes to the environment (either visual or mechanistic changes) unseen in the training phase. The question of generalization in RL is essential to the field’s future both in theory and practice. One proposed solution toward the goal of designing machines that can extrapolate experience across environments and tasks is to learn invariances in a causal graph structure. A key requirement to learn invariances from data may be the possibility to perform and learn from interventions. Work in developmental psychology argues that there is a need to experiment in order to discover causal relationships [81]. This can be modeled as an RL environment, where the agent can discover causal factors through interventions and observing their effects. Furthermore, causal models may allow modeling the environment as a set of underlying ICMs such that, if there is a change in distribution, not all the mechanisms need to be relearned. However, there are still open questions about the right way to think about generalization in RL, the right way to formalize the problem, and the most relevant tasks.

3) Counterfactuals: Counterfactual reasoning has been found to improve the data efficiency of RL algorithms [38], [164] and improve performance [51], and it has been applied to communicate about past experiences in the multiagent setting [69], [241]. These findings are consistent with work in cognitive psychology [65], arguing that counterfactuals allow to reason about the usefulness of past actions and transfer these insights to corresponding behavioral intentions in future scenarios [145], [199], [203].

We argue that future work in RL should consider counterfactual reasoning as a critical component to enable acting in imagined spaces and formulating hypotheses that can be subsequently tested with suitably chosen interventions.

4) Off-Line RL: The success of deep learning methods in the case of supervised learning can be largely attributed to the availability of large data sets and methods that can scale to large amounts of data. In the case of RL, collecting large amounts of high-fidelity diverse data from scratch can be expensive and, hence, becomes a bottleneck. Off-line RL [73], [150] tries to address this concern by learning a policy from a fixed data set of trajectories, without requiring any experimental or interventional data (i.e., without any interaction with the environment). The effective use of observational data (or logged data) may make real-world RL more practical by incorporating diverse prior experiences. To succeed at it, an agent should be able to infer the consequence of different sets of actions compared to those seen during training (i.e., the actions in the logged data), which essentially makes it a counterfactual inference problem. The distribution mismatch between the current policy and the policy that was used to collect offline data makes off-line RL challenging as this requires us to move well beyond the assumption of independently and identically distributed data. Incorporating invariances by factorizing knowledge in terms of ICMs can help make progress toward the off-line RL setting.

F. Scientific Applications

A fundamental question in the application of machine learning in natural sciences is to which extent we can complement our understanding of a physical system with machine learning. One interesting aspect is physics simulation with neural networks [94], which can substantially increase the efficiency of hand-engineered simulators [104], [143], [211], [265], [269]. Significant
out-of-distribution generalization of learned physical simulators may not be necessary if experimental conditions are carefully controlled although the simulator has to be completely retrained if the conditions change.

On the other hand, the lack of systematic experimental conditions may become problematic in other applications, such as health care. One example is personalized medicine, where we may wish to build a model of a patient health state through a multitude of data sources, such as electronic health records and genetic information [66], [109]. However, if we train a clinical system on doctors’ actions in controlled settings, the system will likely provide little additional insight compared to the doctors’ knowledge and may fail in surprising ways when deployed [19]. While it may be useful to automate certain decisions, an understanding of causality may be necessary to recommend treatment options that are personalized and reliable [3], [6], [31], [164], [201], [224], [242], [273].

Causality also has significant potential in helping understand medical phenomena, for example, in the current COVID-19 pandemic, where causal mediation analysis helps disentangle different effects contributing toward case fatality rates when a textbook example of Simpson’s paradox was observed [260].

Another example of a scientific application is in astronomy, where causal models were used to identify exoplanets under the confounding of the instrument. Exoplanets are often detected as they partially occlude their host star when they transit in front of it, causing a slight decrease in brightness. Shared patterns in measurement noise across stars light-years apart can be removed in order to reduce the instrument’s influence on the measurement [218], which is critical especially in the context of partial technical failures as experienced in the Kepler exoplanet search mission. The application of [218] leads to the discovery of 36 planet candidates [71], of which 21 were subsequently validated as bona fide exoplanets [172]. Four years later, astronomers found traces of water in the atmosphere of the exoplanet K2-18b—the first such discovery for an exoplanet in the habitable zone, that is, allowing for liquid water [26], [254]. This planet turned out to be one that had first been detected in [71, exoplanet candidate EPIC 201912552].

G. Multitask Learning and Continual Learning

State-of-the-art AI is relatively narrow, that is, trained to perform specific tasks, as opposed to the broad, versatile intelligence allowing humans to adapt to a wide range of environments and develop a rich set of skills. The human ability to discover robust, invariant high-level concepts and abstractions and to identify causal relationships from observations appears to be one of the key factors allowing for a successful generalization from prior experiences to new, often quite different, “out-of-distribution” settings.

Multitask learning refers to building a system that can solve multiple tasks across different environments [41], [209]. These tasks usually share some common traits. By learning similarities across tasks, a system could utilize the knowledge acquired from previous tasks more efficiently when encountering a new task. One possibility of learning such similarities across tasks is to learn a shared underlying data-generating process as a causal generative model whose components satisfy the SMS hypothesis [219]. In certain cases, causal models adapt faster to sparse interventions in distribution [131], [194].

At the same time, we have clearly come a long way already without explicitly treating the multitask problem as a causal one. Fuelled by abundant data and compute, AI has made remarkable advances in a wide range of applications, from image processing and natural language processing [36] to beating human world champions in games, such as chess, poker, and Go [223], improving medical diagnoses [166], and generating music [57]. A critical question thus arises: why cannot we just train a huge model that learns environments’ dynamics (e.g., in an RL setting) including all possible interventions? After all, distributed representations can generalize to unseen examples, and if we train over a large number of interventions, we may expect that a big neural network will generalize across them. To address this, we make several points. To begin with, if data were not sufficiently diverse (which is an untestable assumption a priori), the worst case error to unseen shifts may still be arbitrarily high (see Section VII-C). While, in the short term, we can often beat “out-of-distribution” benchmarks by training bigger models on bigger data sets, causality offers an important complement. The generalization capabilities of a model are tied to its assumptions (e.g., how the model is structured and how it was trained). The causal approach makes these assumptions more explicit and aligned with our understanding of physics and human cognition, for instance, by relying on the ICM principle. When these assumptions are valid, a learner that does not use them should fare worse than one that does. Furthermore, if we had a model that was successful in all interventions over a certain environment, we may want to use it in different environments that share similar albeit not necessarily identical dynamics. The causal approach and, in particular, the ICM principle, point to the need to decompose knowledge about the world into independent and recomposable pieces (recomposable depending on the interventions or changes in the environment), which suggests more work on modular ML architectures and other ways to enforce the ICM principle in future ML approaches.

At its core, i.i.d. pattern recognition is but a mathematical abstraction, and causality may be essential to most forms of animate learning. Up until now, machine learning has neglected a full integration of causality, and this article argues that it would indeed benefit from integrating causal concepts. We argue that combining the strengths of both fields, that is, current deep learning methods and tools and ideas from causality, may be a necessary step on the path toward versatile AI systems.
VIII. CONCLUSION

In this work, we discussed different levels of models, including causal and statistical ones. We argued that this spectrum builds upon a range of assumptions, both in terms of modeling and data collection. In an effort to bring together causality and machine learning research programs, we first presented a discussion on the fundamentals of causal inference. Second, we discussed how the independent mechanism assumptions and related notions, such as invariance, offer a powerful bias for causal learning. Third, we discussed how causal relations might be learned from observational and interventional data when causal variables are observed. Fourth, we discussed the open problem of causal representation learning, including its relation to the recent interest in the concept of disentangled representations in deep learning. Finally, we discussed how some open research questions in the machine learning community may be better understood and tackled within the causal framework, including SSL, domain generalization, and adversarial robustness.

Based on this discussion, we list some critical areas for future research.

A. Learning Nonlinear Causal Relations at Scale

Not all real-world data are unstructured and the effect of interventions can often be observed, for example, by stratifying the data collection across multiple environments. The approximation abilities of modern machine learning methods may prove useful to model nonlinear causal relations among large numbers of variables. For practical applications, classical tools are not only limited in the linearity assumptions often made, but also in their scalability. The paradigms of metalearning and multitask learning are close to the assumptions and desiderata of causal modeling, and future work should consider: 1) understanding under which conditions nonlinear causal relations can be learned; 2) which training frameworks allow to best exploit the scalability of machine learning approaches; and 3) providing compelling evidence on the advantages over (noncausal) statistical representations in terms of generalization, repurposing, and transfer of causal modules on real-world tasks.

B. Learning Causal Variables

“Disentangled” representations learned by state-of-the-art neural network methods are still distributed in the sense that they are represented in a vector format with an arbitrary ordering in the dimensions. This fixed-format implies that the representation size cannot be dynamically changed; for example, we cannot change the number of objects in a scene. Furthermore, structured and modular representations should also arise when a network is trained for (sets of) specific tasks, not only autoencoding. Different high-level variables may be extracted depending on the task and affordances at hand. Understanding under which conditions causal variables can be recovered could provide insights into which interventions are robust to predictive tasks.

C. Understanding the Biases of Existing Deep Learning Approaches

Scaling to massive data sets and relying on data augmentation and self-supervision have all been successfully explored to improve the robustness of the predictions of deep learning models. It is nontrivial to disentangle the benefits of the individual components, and it is often unclear which “trick” should be used when dealing with a new task, even if we have an intuition about useful invariances. The notion of strong generalization over a specific set of interventions may be used to probe existing methods, training schemes, and data sets in order to build a taxonomy of inductive biases. In particular, it is desirable to understand how design choices in pretraining (e.g., which data sets/tasks) positively impact both transfer and robustness downstream in a causal sense.

D. Learning Causally Correct Models of the World and the Agent

In many real-world RL settings, abstract state representations are not available. Hence, the ability to derive abstract causal variables from high-dimensional, low-level pixel representations and then recover causal graphs is important for causal induction in real-world RL settings. Moreover, building a causal description for both a model of the agent and the environment (world models) should be essential for robust and versatile model-based RL.

Acknowledgment

The authors thank the past and present members of the Tübingen Causality Team, without whose work and insights, this article would not exist, in particular, to Dominik Janzing, Chaochao Lu, and Julius von Kügelgen who gave helpful comments on [217]. The text has also benefited from discussions with Elias Bareinboim, Christoph Bohle, Leon Bottou, Isabelle Guyon, Judea Pearl, and Vladimir Vapnik. The authors would like to thank Wouter van Amsterdam for pointing out typos in the first version. They also thank Thomas Kipf, Klaus Greff, and Alexander d’Amour for the useful discussions. Finally, they thank the thorough anonymous reviewers for highly valuable feedback and suggestions.

REFERENCES


This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.