The Worst of Both Worlds: A Comparative Analysis of Errors in Learning from Data in Psychology and Machine Learning

Jessica Hullman  
Northwestern University  
jhullman@northwestern.edu

Sayash Kapoor  
Princeton University  
sayashk@princeton.edu

Priyanka Nanayakkara  
Northwestern University  
priyankan@u.northwestern.edu

Andrew Gelman  
Columbia University  
gelman@stat.columbia.edu

Arvind Narayanan  
Princeton University  
arvindn@cs.princeton.edu

ABSTRACT
Arguments that machine learning (ML) is facing a reproducibility and replication crisis suggest that some published claims in research cannot be taken at face value. Concerns inspire analogies to the replication crisis affecting the social and medical sciences. A deeper understanding of what reproducibility concerns in supervised ML research have in common with the replication crisis in experimental science puts the new concerns in perspective, and helps researchers avoid “the worst of both worlds,” where ML researchers begin borrowing methodologies from explanatory modeling without understanding their limitations and vice versa. We contribute a comparative analysis of concerns about inductive learning that arise in causal attribution as exemplified in psychology versus predictive modeling as exemplified in ML. We identify common themes in reform discussions, like overreliance on asymptotic theory and non-credible beliefs about reality itself. ML research cannot be taken at face value. Concerns inspire analogies to the replication crisis—published results cannot be reproduced using the same software and data due to unavailable tuning parameters, random seeds, and other configuration settings or computational infrastructure that are not available to outsiders—replication—where re-implementing described methods does not produce the same results due to unacknowledged dependencies, such as specific implementations, and—generalizability or robustness—where methods may work well under certain conditions but fail when applied to new problems or in the world [169], where vulnerability to adversarial manipulations may be costly. For example, the identification of examples by which computer vision models could be tricked into misclassification by manipulations not visible to the human eye [202] has inspired subsequent research proposing a variety of explanations for the apparent brittleness of performance (e.g., [54, 79, 96]). Terms like “alchemy” [123] and “graduate student descent” are used to describe how researchers combine optimizations to often opaque parameters to achieve performance benchmarks. Model performance evaluations are conducted without acknowledging sources of error [3, 99, 138] and can involve data filtering decisions that impact achievable accuracy [33, 137, 138].

Some amount of replication failure is inevitable: the nature of empirical research is to try out ideas that may work in some settings but not others. When claims are published, uncertainty about generalizability is inherent. However, once systemic problems are recognized, corrective actions should be taken, and claims discounted—especially when they cannot be externally reproduced [42, 85, 125].

One way that authors call attention to concerns in ML research is analogizing them to the replication crisis in psychology [19, 36, 110, 115]. While psychologists discussed fundamental issues with conventional approaches to inference as early as the 1960s [50, 148], in the last decade critics brought concerns to the forefront, demonstrating how motivated researchers can obtain false positives under various conditions [75, 76, 192] and that many published conclusions about human behavior in psychology research cannot be replicated [67, 161]. These revelations spur hard questions about what are necessary conditions for science, how to resolve uncertainty about published claims, and how to shift incentives.

CCS CONCEPTS
• Computing methodologies → Learning paradigms: Supervised learning.

KEYWORDS
Machine learning, replication, science reform, generalizability.

ACM Reference Format:

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

AIES ’22, August 1–3, 2022, Oxford, United Kingdom
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM. ACM ISBN 978-1-4503-9247-1/22/08 ... $15.00
https://doi.org/10.1145/3514094.3534196
Despite their focus on predictive modeling (and abundant recent successes in terms of performance on benchmarks, e.g., [71] and adoption in real-world applications, e.g., [145]), fields like AI and ML could learn from psychology’s ongoing attempts to diagnose sources of non-replicability and reform conventional use and reporting of methods in the causally-focused explanatory modeling paradigm prevalent in psychology.\(^1\) Taking a wider perspective on learning failures is well aligned with the idea of integrative modeling, referring to approaches that combine aspects of both paradigms [114, 115, 177, 224]. For example, social scientists might use prediction along with explanation to reduce overfitting to noisy experiment results, while researchers in fields like ML can incorporate explanatory methods to ascertain what a model appears to have learned. Integrative modeling acknowledges how researchers frequently misunderstand the relationship between explanation and prediction, assuming, e.g., that models that succeed in explaining have greater predictive validity [224] than those that appear less psychologically plausible ([106, 191] as cited in [224]) or that a model that achieves high predictive accuracy won’t deviate much from what a human considers to be a plausible decision rule [79]. But to avoid integrative modeling leading to “the worst of both worlds,” researchers will need to understand subtle differences in ways in which inferences can be limited in each paradigm. To date, connections that authors have drawn between these two reform discussions have been piecemeal, leaving it unclear what lessons, if any, might be gained from putting these domains in conversation.

To address this gap, we contribute a detailed comparison of limitations of inference in causally-driven explanatory versus predictive modeling. Our analysis is synthesized from formal and informal arguments made in hundreds of papers we collected through online search, citation tracing, and our involvement in events and scholarly discussions on replication and reproducibility over multiple years. While we surface issues that affect various areas in psychology and ML, we ground our discussion around examples from experimental social psychology, which like ML relies on data reflecting human behavior and uses controlled comparisons to produce claims, and empirical research in supervised discriminative learning (i.e., classification) methods, including deep neural nets (DNNs) that encapsulate many recent concerns.

Our results highlight where concerns across the two domains can stem from similar types of oversights, including overreliance on theory, underspecification of learning goals, non-credible beliefs about real-world data generating processes, overconfidence based in conventional faith in certain procedures (e.g., randomization, test-train splits), and tendencies to reason dichotomously about empirical results. In both fields, claims from learning are implied to generalize outside the specific environment studied (e.g., the input dataset or subject sample, modeling implementation, etc.) but are often impossible to refute due to undisclosed sources of variance in the learning pipeline. We argue in particular that many of the errors recently discussed in ML expose the cracks in long-held beliefs that optimizing predictive accuracy using huge datasets absolves one from having to consider a true data generating process or formally represent uncertainty in performance claims. At the same time, the goals of ML are inherently oriented toward addressing learning failures, suggesting that lessons about irreproducibility could be resolved through further methodological innovation in a way that seems unlikely in social psychology. This assumes, however, that ML researchers take concerns seriously and avoid overconfidence in attempts to reform. We conclude by discussing risks that arise when sources of errors are misdiagnosed and the need to acknowledge the role that human inductive biases play in learning and reform.

2 BACKGROUND

2.1 Anatomy of a learning process

An idealized learning process begins with the formulation of goals (including scientific goals such as understanding what factors influence a particular human behavior, engineering goals such as constructing a better model for machine translation, or policy goals such as estimating effectiveness among different types of patients) and hypotheses. These are not necessarily statistical “hypotheses”; rather, a hypothesis could be that a certain thinking pattern increases the chances of a behavior, or that a certain technical innovation will lead to a better translation system, or that a treatment will be more effective among men than women. Goals and hypotheses lead to steps of data collection and preparation. Researchers specify an observational process to collect information about the latent phenomena of interest from the environment. An observational probe is used to induce explicit observations thought to be sensitive to the target phenomena. For example, psychologists design human subjects experiments using interventions thought to interact with the target phenomena. ML researchers often make use of datasets generated from human produced media and signals of behavior, in the form of digital traces.

An observational process becomes a model by making assumptions about what the observed data represent, namely realizations of random variables with regular variation. The observational model is defined by a model representation, i.e., the model class or functional form that specifies a space of data generating processes (DGP’s, i.e., fitted functions) that might have produced the data. This might be a multiple linear regression functional form in social psychology, or a more DNN architecture in ML (with a specific configuration of network parameters like arrangement into convolutions, activation functions, etc.). Because quantifying and searching all DGPs implied by probability distributions over the observation space tends to be prohibitively complex, learning pipelines often consider a subset or “small world” of model configurations [27], called the hypothesis space of the learner in ML. Model selection or model-based inference describes how a best fit model that is most consistent with the data is determined. This involves defining an objective or loss function measuring the difference between the ground-truth observed outcome for an input and the predicted outcome of a parameterized model configuration (e.g., squared error), as well as an optimization method for searching the space of model configurations to find the fitted function that minimizes loss (e.g., gradient descent, adaptive optimization algorithms, analytical solutions like maximum likelihood estimation (MLE), etc.).

An evaluation may follow to validate the usefulness of what is learned relative to alternative model fits or learning pipelines. Evaluation metrics such as explained variance or log loss can be used

\(^1\)Also known as attribution [73], and typically involving estimation of regression surfaces and assignment of significance to individual predictors.
to summarize overall usefulness of a fitted function. Evaluation metrics may sometimes be implicit, such as when the usefulness of a fitted model is evaluated relative to one’s hypotheses about the data generating process. The learning process culminates in communication of claims in research papers. By “errors in learning,” we refer to issues that arise in this larger process in which a researcher specifies and “solves” a learning problem.

2.2 Goals of learning in social psychology versus machine learning

Social psychology. A primary goal in empirical psychology is to describe the causal underpinnings of human behavior [148, 191, 224]. Researchers identify underpinnings of human behavior [149], predicting a directional difference or association between variables but not the size of the effect. They design observational processes to gather data for testing hypotheses, typically controlled human-subjects experiments that record the thoughts, emotions, or behavior of subjects, under different conditions thought to interact with the latent phenomena of interest. The approximating functions that researchers learn from these observations (often low dimensional linear regressions) are thought to capture key structure in the latent psychological phenomena. Claims about cause and effect hinge on interpreting the parameter values of the fitted function in light of hypotheses and their sampling variation within a statistical testing framework. A function is commonly deemed worthy of interest if its p-value is below a false-positive rate defined in the Neyman-Pearson framework, typically \( \alpha = 0.05 \). Direct claims take the form of statements about novel, statistically significant causal attributions, and have been called “stylized facts” [84, 113] implied by authors to be generally true about human behavior. For example, thinking about old age induces old-like behavior [13].

Machine learning. A primary goal in supervised ML research is to facilitate the learning of functions which achieve high predictive accuracy in tasks like classification. Researchers hypothesize procedures or abstractions that may improve the state-of-the-art (SOTA) in subareas (e.g., natural language processing (NLP), vision), which is captured by benchmarks: abstractly defined tasks (e.g., image classification, machine translation) instantiated with learning problems consisting of datasets (input, output pairs) and an evaluation metric to be used as a scoring function (e.g., accuracy) [138]. Standard methods like using a train-test split and cross validation are designed to ensure good predictive performance of a fitted model on unseen data. Claims in empirical research papers typically report performance of a new learner (i.e., model) on benchmarks, compared to baselines representing the prior SOTA. Formal proofs of the statistical properties of new methods are also common.

3 THREATS TO LEARNING IN SOCIAL PSYCHOLOGY AND MACHINE LEARNING

We describe threats to valid learning according to whether they involve data selection and preparation, model development (including choosing a representation and a model selection and evaluation approach), and communication of results in a research paper.

3.1 Data collection and preparation

Social psychology. High measurement error relative to signal, unacknowledged flexibility in defining data inputs, underspecified or non-representative subject samples, and underspecification of stimuli generation, and other “design freedoms” can threaten the validity of conclusions drawn in empirical psychology research.

The design of many psychology experiments implies that researchers do not grasp the implications of using small samples and noisy measurements to draw inferences about effects that are a priori likely to be small. For example, a thought-to-be pervasive belief is that if an experiment registers a “statistically significant” effect on a small sample, then that effect will necessarily remain significant with a larger sample [42, 192]. In reality, with a lower powered study, not only is there a lower probability of finding a true effect of a given size, but there is a lower probability that an observed effect which passes a significance threshold actually reflects a true effect that will appear under replication [42]. Under low power, estimates of observed effects will tend to reflect sampling error that derives from the limited size of the sample relative to a target population, and forms of measurement error [141], such as random variation due to noise in taking measurements that produces a difference between observed and true values. Studies are “dead on arrival” when standard error due to measurement and sampling variation is large relative to any plausible effect size [91].

Inherent flexibility in how a researcher specifies an analysis is a different type of threat. A “researcher degrees of freedom” or “garden of forking paths” metaphor [88, 192] suggests that human tendencies toward self-serving interpretations of ambiguous evidence (e.g., [11, 58] as cited in [192]), make researchers likely to draw conclusions that verify their hypotheses. Given an outcome of interest (e.g., self-reported political preference), an analyst may bias results toward a preferred conclusion by selecting data transformations and outlier removal processes, or choosing between different predictor variables or ways of operationalizing the outcome variable, conditional on seeing the results of these choices, without necessarily recognizing they are doing anything improper. More broadly, when a researcher can tweak the design of experiment conditions with feedback through pilot experiments via the design of stimuli, instructions, and elicitation instruments, they may gravitate toward designs that exaggerate effects in some conditions, resulting in a form of procedural overfitting.

Scholars have pointed to study results not being reproducible because they use non-representative samples of a target population, such as convenience samples of university students from western educated industrialized rich democratic (WEIRD) countries [112]. As researchers have become more accustomed to the importance of statistical power and representative samples, online recruitment of participants in social psychology [183] has increased. However, it is unclear that sample homogeneity is addressed by online samples [46] and this trend has led to greater use of self-reported measures [183] that contribute additional noise. More generally, failure to recognize the implications of non-random sampling can lead to a “big data paradox” of overconfidence as sample size increases [151]. Another fundamental but often overlooked issue concerns how psychologists often leave the target population of their inferences unspecified [93], making it ambiguous what is being learned at all.
Machine learning. Standardization of benchmarks and the prohibitive cost of amassing large datasets means that researchers often rely on existing datasets [108, 200], typically obtained through crowdsourced annotation and web-scale data (e.g., [61, 135]). Similar to psychology, factors like choosing how to transform data after seeing results, the use of non-representative samples, and underspecification of the population captured in data threaten the validity of claims. More frequently discussed issues include the differential effects of non-random measurement error on real world outcomes when a model is deployed and the way that a “good” predictive model can perpetuate forms of historical bias like stereotypes.

Recent work in ML points to analogous concerns to psychology in recent acknowledgement of flexibility in data transformation, such as in filtering data in ways that simplify a prediction problem (e.g., removing translation artifacts in machine translation to improve prediction accuracy [137] as cited in [138]).

Non-representative samples are also a concern, including violations of the assumption that the development distribution from which the training and test data are presumed to be randomly drawn is the same as the deployment distribution from which samples will be drawn in real-world applications [14, 165, 201]. “Representation bias” [201] involves development data that under-represent some parts of the input space of an ML algorithm, leading to higher error rates for less-represented instances in the input space (e.g., [41, 164, 227]). Suresh and Guttag [201] define this bias as a positive value for a measure of divergence between the probability distribution over the input space and the true distribution, noting that it can occur simply as a result of random sampling from a distribution where some groups are in the minority. Others describe how error in the (often unreported [78]) labeling process used to construct ground truth can lead to overfitting [38, 160], as well as how data preparation steps lose information whenever majority-rule is used to construct a ground truth without preserving information about label distributions (e.g., describing variance across annotators) [57, 98].

However, criticism of data practices in ML often focuses on systematic measurement error (i.e., bias) in collected data that threatens construct validity: whether the measurement is actually capturing the intended concept. “Measurement bias” [201] has been used to refer to differential measurement error [211], where a measurement proxy is generated differently across groups due to differing granularity or quality of data across groups, or reduction of complex target category (e.g., academic success) to a small number of proxies that favor certain groups over others (e.g., [134] as cited in [201]). Jacobs and Wallach [126] attribute many misleading claims in the fairness literature in ML to unacknowledged mismatches between unobservable theoretical constructs in ML applications (e.g., risk of recidivism, patient benefit) and the measurement proxies that researchers often tend to assume capture them, and suggest the use of latent variable models to formally specify assumptions.

A novel concern about measurement bias in ML relative to psychology occurs when biased input data are used to train a model and contribute to undesirable social norms. Data may record historical biases [201] (e.g., training a model to recognize successful applicants on data where women were admitted less due to bias). “Harms of representation” [1, 52] refers to how model predictions can reinforce potentially harmful stereotypes when trained on data exhibiting bias. For example, returning pictures of only white males on a Google search for CEO reinforces notions that other groups are not as appropriate for CEO positions [132]. The fact that ML is often intended for prescriptive use in the world, rather than descriptive use as in psychology research helps explain the prevalence of these concerns and the emphasis on systematic measurement error.

Finally, data concerns in ML increasingly refer to forms of underspecification of population details and underacknowledgment of the constructed nature of data, instead taking data as given [20, 78, 122, 186]. These concerns also imply that real-world harms may result from practices that extract away the subjective judgments, biases, and contingent contexts involved in dataset production [165].

3.2 Model representation

Learning from data requires selecting a model representation, a formal representation that defines what functions can be learned.

Social psychology. Researchers commonly overlook the importance that the small world of model configurations they explore captures or well approximates the true DGP for valid inference, hold unrealistic views about the separability of large effects in the world, and tend to incorporate prior knowledge into modeling informally rather than explicitly.

When modeling a latent psychological phenomenon, often via simple measures of correlation and linear parametric models [30, 31], researchers implicitly assume that there is a true DGP that exactly captures how the target arises as a function of other factors thought to influence it. Once an observational model is defined, inference is confined to the mathematical narratives represented by these functions [89]. However, the validity of claims made about causal effects by following this process depend upon judicious choices about how to represent structure in the true DGP in the constrained small world model space, which psychology researchers often overlook [213].

A first complication arises from the fact that inference is more straightforward when the true DGP is included in the small world of configurations under consideration [26]. However, the sorts of human behaviors psychologists tend to target are thought to be conceptualizable but too complicated to specify explicitly, or not even conceptualizable [213]. Under these conditions, the validity of conventional interpretations of fitted models depends on the observational model faithfully approximating the true DGP [89].

However, this is not the case when a model is structurally misspecified, meaning the fitted models do not adequately capture the true causal structure and/or the functional form of the relationships between variables in the true DGP [213]. For example, if the DGP in a psychology study can be described as a weighted sum of the set of input variables that are represented in the chosen functional form, and all of these predictors are exogenous (i.e., completely independent), then parameters estimated using ordinary least squares can be interpreted according to convention as information about the target phenomena (e.g., comparing two items that differ by one unit in predictor x while being the same in all other predictors will differ in y by θ, on average). However, when the true DGP is more complex than the functional form, the choice of which potential confounding variables one measures and includes in the regression equation becomes important. Not including variables that influence a regressor and the outcome [7] or including variables that could in
### Social Psychology

| Data selection and preparation | • High measurement error relative to the size of effects being studied [15, 62, 141]  
• Data transformations decided contingent on (NHST) results [88, 192]  
• Non-representative [112, 151] or underdefined samples [93]; insufficient stimuli sampling [92, 218, 223]  
• Small samples and noisy measurements (low power) leading to biased estimates [42] |
| Model representation | • Overreliance on models and designs with good asymptotic guarantees [159]  
• No explicit representation of prior/domain knowledge [80, 89]  
• Inappropriate expectations [49, 82, 223] in light of crud factor [149, 162]; belief in many nudging factors with large consistent effects on outcome [209]  
• Unacknowledged multiplicity of solutions [224]  
• Structural misspecification [144, 213] |
| Model selection and evaluation | • Implicit optimization for statistical significance [85, 87, 88, 97, 121, 136]  
• Inference as black box [93, 136, 217]; Not motivating choice of estimator or optimization for particular inference goal [24, 215]  
• Misunderstanding/misusing ideas of statistical significance [81, 102, 120, 121, 214]  
• Multiple comparisons problem [86] |
| Communication of claims | • Unwarranted speculation about what evidence a p value provides [204]  
• Overgeneralization (i.e., beyond studied population) [60, 105, 178, 194, 223]  
• Unavailable data and code [83, 117, 153]  
• Not acknowledging having explored multiple analyses-conditioned on data [86, 192]  
• Inaccurate descriptions of what p values mean [4, 28, 90, 204] |
| Machine Learning | • Differential measurement error (e.g., across social groups) [41, 164, 201, 227] which is not modeled [126, 134]  
• Label errors [38, 160] and disagreement [57, 98]  
• Data transformations decided contingent on performance comparisons [33, 137]  
• Underrepresentation of portions of input space in training data [14, 165, 201]  
• Input data too huge to understand [20, 165] |

#### Table 1: Overview of learning concerns, roughly ordered to emphasize similarities across social psychology and ML.

Principle be affected by experimental manipulations (and hence represent outcome variables themselves [51]) cause the conventional interpretation of the fitted parameter values not to hold. However, researchers seldom acknowledge these limitations.

Researchers often choose designs based on a preference for simpler models. Perhaps the most common example is preferring between-subject designs based on their asymptotic properties: as the size of the (random) sample increases toward the population size, a between-subjects design provides a simpler procedure for estimating average treatment effects relative to a within-subjects design, which requires estimating carryover effects between treatments experienced by the same individual [159]. However, high variation between people can lead to poor estimates of average treatment effects if the treatment interacts with background variables associated with differences in individuals and contexts [144, 159].

More generally, psychology researchers have been criticized for estimating effects as if they are constant rather than assuming they will vary across people or contexts [82]. This can manifest, for example, as model specifications that ignore the importance of modeling variation in stimuli and other experimental conditions as well as subjects [223] (e.g., a “fixed effect fallacy” [49]).

Tendencies to overlook important sources of variation in modeling are implied by Meehl’s conception of the “crud factor” [149, 162], which emphasizes how causal attribution using constrained model spaces to approximate a highly complex true DGP is fundamentally challenged by the prevalence of “real and replicable correlations” reflecting “true, but complex, multivariate and non-theorized causal relationships” between all variables [162]. Problems arise when researchers overlook model misspecification due to conventional but questionable beliefs about reality. For example, a tendency toward reporting model fits suggesting that novel yet seemingly trivial “nudging” factors (e.g., whether or not someone is menstruating [70] or whether there was a recent shark attack [2]) have large and consistent effects on the same outcomes (e.g., voting behavior) overlooks the fact that if such effects were large, we should expect them to interact in complex ways. Hence, we should expect it to be very difficult to observe stable and replicable effects [209].
In this way, choices of model representation (i.e., low dimensional linear regressions) are not fully consistent with prior knowledge. Conventional approaches to estimating an effect of interest are also memoryless in the sense that even when prior estimates of an effect of interest are available, e.g., from past experiments, they are generally not incorporated in the model representation. Combined with incentives to publish surprising results [74, 185] and the inflated probability of observed effects to be overestimates in small sample size studies (Section 3.1), this can result in published effects that seem suspiciously big in light of prior domain knowledge.

**Machine learning.** In theory, optimizing for predictive accuracy does not require well-approximating a true DGP. However, researchers commonly assume that unseen data are drawn from the same distribution as training data and use asymptotics to motivate model choice, leading to unrealistic beliefs about the predictability of real world processes. Threats also arise from failures to explicitly represent a priori human expectations about what predictors are valid for a task, and a convergence on hard-to-analyze models that combine pre-trained representations with domain-specific data.

The biggest point of contrast between representations in supervised learning in ML and social psychology is that the former traditionally do not assume that the learning process is “realizable” [181] in the sense that the true DGP is in the set of learnable functions (or hypothesis space), nor even that the fitted function approximates the structure of the true DGP. Instead, the goal of learning can be formulated as identifying a function with error that can be guaranteed to fall within some bound of the best possible predictor over possible samples [210]. Choosing a representation (i.e., hypothesis space) in theory means reasoning about the inductive biases (i.e., properties of the predictors) it will return in light of prior knowledge, but in practice theoretical guarantees (e.g., worst-case bounds) on convergence or generalization ability have driven representation choices. This can lead, as in psychology, to use of models in cases where asymptotic assumptions don’t apply [65]. Or, as in the case of much recent DL research, a more empirical, performance-driven approach uses achievable performance as the primary driver of model choice [174].

One of the most commonly cited deficiencies attributed to model representations in applied ML involves assuming a static relationship between the predictor variables and the outcome [212], which supports conventions like shuffling input data to create training and test sets [9]. This assumption makes models vulnerable to concept drift [220] (a.k.a. covariate shift [29] or distribution or dataset shift [198]), where predictions are inaccurate post-hoc due to non-stationarity in the real-world relationship between the inputs and outputs due to temporal changes (e.g., [143]), behavioral reactions (e.g., [167]), or other unforeseen dynamics [170]. Under conventional “distribution unawareness,” it also becomes difficult to distinguish when unexpected errors arise from distribution shift versus inefficiencies in the learning pipeline [23]. Distribution shift can lead to poorly calibrated estimates of the uncertainty of model performance [163], similar to how choosing estimators by convention rather than guided by one’s inference goal (see Section 3.3) biases uncertainty estimates for effects observed in psych experiments.

Distribution shift motivates greater focus on how different models fare at out-of-distribution (OOD) error and their robustness to adversarial manipulation, i.e., small changes to an input in feature space that dramatically change the predicted output (e.g., [16, 44, 179, 202, 207]). Recent results related to adversarial nonrobustness [124], underspecification [54], shortcut learning [79], simplicity bias [190], and competency problems [77] suggest that beliefs about the true DGP in predictive modeling as in ML are not necessarily as distinct from explanatory, attribution-oriented modeling as past comparative accounts (e.g., [39]) imply.

For example, one understanding of concept drift that we can relate to the so-called crud factor in psychology is that the concept of interest (or target task) in an ML pipeline for discriminative learning often depends on a complex combination of features that are not explicitly represented in the model. Geirhos et al. [79] use “shortcut learning” to refer to a tendency for ML models to learn simple decision rules (e.g., [10, 129, 147]) that perform well on standard benchmarks. While these features represent “real” correlations, the problem is that singular predictive features mined in training data often do not perform as well in more challenging testing situations, where a human might naturally expect successful performance to require combinations of features (e.g., derived from several different object attributes in object recognition). Shortcut learning and related vulnerabilities to adversarial manipulation imply not a failure in learning from a modeling standpoint, nor even a failure of a fitted function to generalize [79], but a mismatch between a human’s conception of critical, stable properties that predict under the true DGP and those that drive the predictions of the fitted model [54, 79, 124].

A related theory representing a symptom of predictive multiplicity is underspecification [54]: specifically, a failure to represent in the learning pipeline which inductive biases are more desirable to constrain learning. Underspecification occurs when predictors with equivalent performance on i.i.d. data from the same distribution as training degrade non-uniformly in performance when probed along practically relevant dimensions [54]. Underspecification is distinct from forms of distribution shift that may give rise to shortcut learning, such as the presence of spurious features in the training data that are not associated with the label in other settings. Instead, it captures how a single learning problem specification can support many near-optimal solutions but which might have different properties along some human relevant dimensions like fairness or interpretability [180].

A common approach to overcoming poor generalization of a model is to combine multiple representations. Representation learning—automated, untrained learning of input representations (i.e., generic priors) on huge datasets that capture structure in domains like language or vision—reduces the difficulty of achieving high accuracy in domains where labeled data is costly [22]. “Fine-tuning” pretrained “foundation” models [32] for domain-specific applications has become standard practice based on the performance that can be achieved over conventional domain-specific learning pipelines [104, 200, 221]. Though training on highly diverse input data tends to provide foundation models with inductive biases that improve extrapolation, a challenge is that fine-tuning performance can be highly sensitive to how poorly-understood parameters are set, making results hard to replicate [64]. For example, the robustness of a fine-tuned model has been found to vary considerably under small changes to hyperparameters [221]. Related is a concern
that the convergence in deep learning research around large DNN model architectures with minimal task-specific parameters [32] doubles down on an approach that imposes unreasonable environmental [20, 199] and research opportunity costs [20].

More generally, understanding the implications of model selection is complex for DNNs, where classical theory falls short of explaining the generalization performance (e.g., [17, 18, 55, 127, 226]). This has motivated lines of theoretical work that explore different explanations of phenomena like “double descent” [17], where the generalization performance of a deep model continues to improve even after it has achieved zero loss on (or perfectly interpolated) the training data. For example, some analyze the properties of over-parameterized linear regressions [55].

### 3.3 Model selection and evaluation

Model-based inference involves explicit and implicit choices of objective function, optimization approach, and evaluation metric.

**Social psychology.** Claims made in social psychology research are threatened when researchers treat conventional approaches to model-based inference as a black box for consuming data and outputting inferences [12, 93, 136], and by researchers’ implicit use of statistical significance alone as a criterion for deciding what to report.

It is relatively rare for psychology research contributions to include explicit motivation for the estimators and loss functions used in modeling. Such “inference by convention” can produce misleading claims without outright cheating or motivated reasoning similar to how blindly preferring between-subjects designs can. For example, conventional use of maximum likelihood estimators based on their consistency [217] may lead researchers to overlook critical assumptions required for these estimators to be well-calibrated (i.e., have sampling distributions which are asymptotically normal). Analytical approaches to optimization bring convenience, but commonly-used approaches to model fitting and selection tend to be based on pre-experimental guarantees (i.e., before data are collected), which cannot guarantee that they will be appropriate (e.g., well-calibrated) on a particular dataset [24, 215].

A different source of misleading claims is the use of statistical significance as a coarse objective function. Implicit optimization for significance, in which researchers are essentially searching through a garden of forking paths for specifications that achieve significance as a sort of quasi-optimization approach [88], means that conventional interpretations of fitted models and statistical tests on parameter estimates will not hold. For example, the multiple comparisons problem, in which researchers neglect to control for data-dependent selection in what they report, alters the statistical properties of estimates and tests [86]. At the highest level, bias affects the published record when researchers decide whether to report results based on the significance levels [85, 185]. Using “statistical significance” as an implicit objective does not line up with scientific goals (e.g., [81, 102, 120, 121, 214]). For example, the use of \( p \)-values and statistical significance in psychology research is described as fundamentally confused in that rejection of straw-man null hypotheses is inappropriately taken as evidence in favor of researchers’ preferred alternatives [97, 121, 136]. In other words, hypothesis testing can sometimes be used as a sort of “truth mill” in psychology [85, 87].

Related problems include not acknowledging that as a random variable, \( p \) can vary considerably even under idealized replication [34, 90, 97, 154, 189], such that the difference between significant and not significant is not itself significant. Researchers also overlook the fact that for \( p \) to be a valid estimate of the probability of observing an effect as large or larger than that seen, all assumptions about the test and observational process must hold [5, 103, 171].

**Machine learning.** Claims are often made in ML research without acknowledging that they depend critically on choices of hyperparameters, initial conditions, and other configuration details that directly influence performance in non-convex optimization. Researchers also may exploit flexibility in designing performance comparisons in order to achieve superior performance for their contributed approach relative to alternatives [114, 188].

In contrast to loss functions in simple regression models, ML models tend to have high dimensional non-convex loss. While this does not necessarily prevent generalization [48] it makes solutions like saddle points, which can give the illusion of a satisfactory local minimum, of greater concern [56, 184]. Optimizers—algorithms that prescribe how to update parameter values like weights during inference to reduce the value of the objective on the training data—are critical to the accuracy gains seen in recent years. However, to make non-convex optimization tractable requires setting various opaque hyperparameters and initial conditions that influence how the loss landscape is traversed [47, 94, 187].

For an optimization approach like stochastic gradient descent (SGD), hyperparameters like the learning rate affect how quickly it learns the local optima of a function: too high a rate means the function cannot converge, too low and it may require too long [36]. Adaptive optimizers (e.g., Adagrad, Adam) allow hyperparameters like learning rate to vary for each training parameter, inducing a new dynamical system with each run and complicating attempts to explain what parts of a pipeline improved performance.

Hyperparameter tuning is also a computationally expensive task [206], inducing uncertainty about how a solution might differ under a larger computational budget or different parameter settings. Some recent work finds that given a fixed computational budget, choosing the best optimizer for a task with the default parameters performs about as well as choosing any widely-used optimizer and tuning its hyperparameters, questioning claims of state-of-the-art performance of newly introduced optimizers across tasks [187]. Similarly, sufficient hyperparameter optimization can mostly eliminate claimed performance differences in generative adversarial networks (GANs) [142], and better hyperparameter tuning on baseline implementations can eliminate evidence of performance advantages of new learning methods [111, 150]. Liao et al. [138] use the broader term “implementation variation” to refer to how variations in how inference techniques are implemented—including use of specific software frameworks and libraries, metric scores, and implementation “tricks” [6, 111]—can affect their performance in evaluations. A related concern in subareas like reinforcement learning is when researchers overlook sources of inherent stochasticity in the training process and evaluation environment [133, 155, 219].

Other inference concerns pertain to the external validity of the functions that are learned: will they predict well on unseen data? In the absence of a theoretical foundation for understanding DNN performance, exploratory empirical research aims to identify proxies
for properties like learnability and generalizability (e.g., [127, 226]). Recent results show how counter to classical expectations about overfitting, minimizing training error without explicit regularization over overparameterized models tends to result in good generalization [158, 195, 226], driving a new theoretical agenda aimed at disentangling optimization methods and statistical properties of the solutions they find. Some emergent properties have been criticized. Related to shortcut learning, SGD has been shown to exhibit “simplicity bias”—a preference for learning simple predictors first, resulting in neural nets relying exclusively on the simplest features, for example, image color and texture, and remaining invariant to complex predictive features, for example, object shape [130, 190].

Other concerns with external validity arise when an explicitly chosen objective function is not a good proxy for the metric of interest in using the models, called “loss-metric misalignment” and threatening generalization [119]. For example, cross-entropy loss is often used as a loss function, whereas the evaluation metric of interest is often classification error or AUCPR. More generally, reporting single scalar error measures by convention overlooks important error variation (e.g., [69]).

Internal and external validity is threatened by leakage—broadly, using information from the test data in training—paralleling the reuse of data for choosing and evaluating a model’s fit in psychology. Leakage can arise when a single CV procedure is used for model tuning and estimating error at once [45, 109, 116]. Failure to carefully consider which steps involved in training should be performed on each fold during CV can bias error estimates on test data [109], as can contaminating the procedure with future data in time series applications [25]. More generally, using CV for performance evaluation has been shown to lead to overoptimistic results in the presence of dependencies between the training and test set under certain conditions [72, 146], not unlike how low-power experiments lead to overestimates of effects in psychology.

Other issues occur in performance comparisons of models or algorithms. Similar to data issues in psychology, sampling error can be overlooked, including low power in performance comparisons [43] and failure to acknowledge that performance estimates on the standard train-test splits common in benchmark datasets may not hold for randomly created train-test splits [99].

Finally, implicit optimization for good performance results can also occur in ML. Improving performance on benchmark datasets, which have been thought to have caused most major ML research breakthroughs in the last 50 years [66], is how researchers showcase improvement in model performance to get published in top conferences and journals [172, 188] across ML subareas (e.g., [61, 118, 216]). This can create incentives for researchers to implicitly optimize inference around a goal of seeing their new technique rank best in performance in an evaluation, such as selectively reporting results to highlight the best accuracy achieved (Section 4), choosing among performance measures conditional on results, or failing to acknowledge how simpler baselines perform relative to a new approach (e.g., how well the “language prior,” the prior distribution over labels [101], performs in a popular visual question answering task (VQA) [8]). Attempts to use OOD data to improve task performance are not valid when researchers rely on explicit knowledge of how the OOD splits were constructed or use the OOD test set for model validation [207].

4 COMMUNICATION OF CLAIMS

Sources of error can remain unacknowledged due to communication norms that suppress uncertainty and limit reproducibility.

Social psychology. The contribution of a social psychology experiment can be framed as a stylized fact: a statement presumed generally true and replicable [84, 113] about some aspect of the world. Results are used to motivate broad claims [60], with deficiencies attributable to authors failing to acknowledge exploration of multiple analysis paths contingent on the data, and tending to downplay inherent dependencies and uncertainty when describing results.

Because stylized facts derive from the results of experiments in laboratory-like environments, often on non-representative samples [84], credible reporting would emphasize the specific conditions studied [194]. Instead, however, researchers routinely state their findings in broad terms in articles, referring to how an intervention or trait affects “people” or entire groups [60, 105, 178], not acknowledging potential variation untested by theory and data.

Authors can perpetuate p-value fallacies when they write about effects as if present or absent (e.g., [28]) or overinterpret alternative hypotheses [204]. Or they may imply that a lack of significance is evidence of an absence of effect [4, 28] or that there is a significant difference between significant and non-significant results [90].

Finally, while sharing of data and analysis code has increased in psychology in recent years, many authors have not adopted such sharing (e.g., [205]). When authors don’t publish data or analysis code they used to arrive at a conclusion, readers cannot as easily identify problems or replicate the work, potentially slowing the rate at which errors that invalidate claims are caught [83, 117, 153].

Machine learning. Communication concerns in ML include tendencies to not report trial and error over the modeling pipeline and evaluation metrics (leading to biased claims about model performance) and to downplay dependencies and uncertainty affecting performance.

ML researchers often report point estimates of performance without quantifying uncertainty [3, 138, 173] or reporting key inputs such as hyperparameter and computational budget settings in non-convex optimization. This can result in performance results for which the source of empirical gains is unclear or misattributed [140]. As examples, authors often do not report the number of models trained and the negative results found before the one they highlight is selected [3, 188]. Authors may cut corners since computing uncertainty and variance in ML models can incur significant computational costs, especially for large ML models [3, 36]. When not presented along with an estimate of the uncertainty of model performance arising from sources of variation like the choice of train-test split [99], the computational budget [63], the choice of hyperparameter values, and the random initialization of ML models [47, 142, 187], point estimates of performance represent the best-case rather than expected model performance. Worse, researchers sometimes apply CV to tune a model then report the best performing model’s error on the training set (i.e., the “apparent error”) as if it were cross-validated error [157].

As with psychology, researchers may be tempted to speculate about causes without couching them in speculative terms [140]. Overgeneralization occurs from the loose connection between a task (e.g., reading comprehension, image classification) given in colloquial and anthropomorphic terms as what a model has learned
to do, and a more specific definition of the problem [138, 140] for which publishable results were achieved. For example, using “reading comprehension” to refer to a process is misleading when the model may not have used what a human would call critical information, like the text it is “comprehending” [131] (Section 3.3). More broadly, claims about performance are rarely evaluated in the context of relevant real-world applications [138].

ML faces analogous issues to the lack of open data and code in social psychology [68, 99, 107, 182, 197]. Details about dataset limitations that can threaten external validity [20, 78, 165] are often unreported in ML literature (Section 3.1), perhaps because new techniques for model creation have historically been valued over documenting datasets [186]. As in psychology, checking computational reproducibility of results requires making the complete code and data available with published papers [40]. Recent work attempts reproducibility checks, documentation, community challenges, and workshops [78, 152, 169]. However, while assessing replication in the social sciences is not trivial (e.g., [196]), a somewhat unique challenge in ML is that with the creation and widespread use of large ML models requiring significant computational resources [20], especially in NLP tasks, it becomes impossible for many researchers to even attempt replicating certain results.

5 IMPLICATIONS: WHAT CAN WE LEARN FROM THIS COMPARISON?

As researchers move toward integrative modeling, they should grasp common blind spots; the summary in Table 1 roughly orders issues to emphasize where concerns overlap between the two fields.

We see evidence of different ways in which researchers place undue confidence in particular statistical methods. In ML, the use of a train/test split and cross validation can give the illusion that the inherent inability to know performance on unseen data is manageable. In social psych, belief in the power of randomized sampling and statistical testing leads researchers to overlook the importance of satisfying other assumptions or modeling other forms of variation, like in sampling stimuli. Motivating choices like model representation using asymptotic theory without considering its applicability to the specific inference problem is conventional. In both cases, researchers’ trust in methods is undergirded by unrealistic expectations about the predictability of real-world behavior and other phenomena. Social psychologists ignore the “crud factor” [148] and improbability that multiple predictors thought to have large effects on the same outcome would not also correlate with one another [209]. ML researchers seem to embrace the crud factor by recognizing the importance of using many predictors to avoid overfitting when the signal from any one predictor is likely to be small [55], but have been slow to part with i.i.d. assumptions.

Norms around what is publishable in each field incentivize researchers to hack results to meet implicit objectives such as statistical significance or better-than-SOTA performance, to the detriment of practical significance or external validity. Important dependencies in the analysis process—from types of data filtering and reuse to unacknowledged computational budgets or unspecified populations—are often overlooked, so that results do not generalize as assumed. Overgeneralization and suppression of uncertainty via binary statements—about the presence of effects or rank of model performance relative to baselines—are common in reporting results.

5.1 Irrefutable claims

On a deeper level, claims researchers are making in both fields appear to be irrefutable both by design and convention. In social psychology, this manifests as papers that set out to confirm hypotheses that associations will exist, or be in a certain direction, rather than mechanistic accounts that enable more specific predictions. When hypotheses provide only weak constraints on researchers’ ability to find confirming evidence and there is flexibility in the analysis process (not to mention incentives to publish positive evidence on often counterintuitive effects [74, 185]), “false positive psychology” [192] is not a surprising result. Consider how much more difficult, even impossible, it for those who wish to refute, rather than support, a given theory: showing no association, for example, means providing evidence for a point prediction of null effect. At the same time, in the absence of well-motivated stimuli sampling strategies, defined target populations, and attempts to model other sources of contextual variation, assuming that claims made about any particular parameter estimates obtained through analyzing experiment results generalize beyond that particular set of participants, stimuli, etc. is not credible.

Turning to ML, many reproducibility failures seem to derive from a similar tolerance for irrefutable contributions, manifesting as a confusion between engineering artifacts and scientific knowledge. Consider a typical supervised ML paper that shows that an innovative algorithm, architecture, or model achieves some accuracy on a performance claim of the given algorithm on the dataset, because the population from which benchmark datasets are drawn are rarely specified to the detail needed for another sample to be drawn [128]. Attempts to collect a different sample from an implied population to refute claims are rare; when they have been attempted, researchers have found that the original claims no longer hold [175]. Further, when researchers have tried to compare model performance across benchmark datasets, they have found that results on one benchmark rarely generalize to another, and can be fragile [59, 208].

At a higher level, analogies between human and artificial intelligence are embedded in AI culture, but without specifying the neurocomputational processing involved in cognition [176], whether ML approaches capture key aspects of human consciousness (e.g., [100]) or new algorithms intended to instantiate human-like mechanisms (e.g., [21]) succeed in a human-like way is speculative.

The acceptance of non-refutable research claims as research contributions, as in social psychology, creates a culture in which other methodological issues amplify the difficulty of building generalizable knowledge. Hubris from beliefs that big data renders modeling requirements like uncertainty quantification unnecessary [35, 59, 139], a lack of rigor in evaluation [138, 188], and over-reliance on theory [95, 140] may leave ML plagued with reproducibility and generalization issues. One potential bright spot lies in widespread recognition that the field is lacking foundational statistical theory to explain DNN performance. This could naturally encourage a more cautious and empirical mindset among
researchers, but only if pressures to make bold claims from structural incentives that encourage “planting one’s flag” before others do [188] don’t outweigh the trend toward embracing uncertainty.

5.2 Latent expectations versus reality

Characterizing the conventions that give rise to irrefutable claims as forms of underspecification—meaning that some aspect of the learning problem has not been formalized to an extent that allows it to be solved—might help point researchers toward new methods to address what is missing. In particular, the role of human expectations in defining “success” in learning has been implicit, but innovations are often driven by making these expectations explicit.

Colloquially, many ML methods are assumed to free researchers from theorizing how well a fitted function captures critical structure in the true DGP. Yet, many weaknesses being identified suggest that the reality of non i.i.d. test data is pushing ML researchers in “purely” predictive areas toward philosophies underlying explanation. Recent definitions of underspecification [54], shortcut learning [79], adversarial vulnerability [124], etc. motivate the need to impose more constraints on what is learned, and the most natural source is the human who assesses and interprets the results.

In social psychology, DGPs are modeled, if only as a symptom of using conventional inference. However, we see a displacement of prior knowledge in designing and interpreting experiments, where a priori expectations about how big an effect could be are often overlooked. There is also a failure to acknowledge how the styles of research the field rewards, such as showing that many small interventions can have large effects on a class of outcomes, are incompatible with common sense expectations of correlated effects.

There is little reason to believe that taking steps toward integrative modeling will greatly improve practice if researchers fail to actively monitor what new methods help them learn for the issues listed in Table 1. The worst of both worlds would result if instead they assume that any use of integrative approaches must increase rigor, because “now we do statistical testing,” “now we do human-subjects experiments,” or “now we use a test/train split.”

Another bright spot in times of methodological crisis is that when mismatch is recognized, it can lead to new technical innovations. Paradoxically, striving to identify a single foolproof solution to a recognized learning problem can drive new techniques to close the gap between expectations and reality. For example, in ML recognizing the “brittleness” of deep learning models in light of human perceptions of learning has led to major improvements to generalization from new approaches to adversarial robustness. ML may have an advantage over psychology in addressing reproducibility problems in that a “cat and mouse” dynamic characterizes many recent successes, where evaluative work is followed by clever changes to the definition of a learning problem or pipeline that overcome that weakness. Perhaps the most important question for modern AI and ML is what, if any, forms of mismatch between human expectations and model behavior cannot be solved through a reframing of the learning problem to find beneficial new “hacks.”

5.3 Epistemological gaps and rhetorical risks

It is natural for fields to amass signals thought to be proxies of trustworthiness to enable judging work at the time of publication, when how well a claim replicates or generalizes is not known. However, a fundamental challenge in doing this is the need for reformers to recognize the incompleteness of their own knowledge.

Consider how irrefutable theories and claims induce greater dependence on imperfect ways of validating claims. In social psychology, replication is an indirect test for whether effects persist under the same or similar conditions. However, experts do not always agree on what constitutes successful replication [166], and intuitions can be proven wrong. For example, under a formal definition of a study’s reproducibility rate, reproducing experimental results does not necessarily indicate a “true” effect, and vice versa for a “false” effect [62]. In ML, tests are similarly indirect, but the stakes often higher: when an approach fails to perform as expected in the world, researchers may scrutinize the original claims, but at the expense of those affected in deployment. Progress can be had to judge due to the speed of discovery [37] and conflicting valuations of standard approaches like benchmarks (e.g., [172, 222]).

There is a need to accurately diagnose the fundamental problems, rather than symptoms only, and avoid the sort of part-for-whole substitution in reformation that drive methodological overconfidence. As fields work toward consensus views on errors, uncertainty must be embraced. For example, debates over what core problems pre-registration addresses point to the challenge of determining when a given reform should have privileged status [156, 193, 203].

Sociological issues also arise when researchers believe good generalization can be achieved via a singular universal method of statistical inference [93]. It can be that more careful researchers tend to use more sophisticated methods, which will show up as a correlation between methodological sophistication and the quality of research—but this can also create an opening for methods to be used as a signal of research quality even when that is not the case. For example, it makes sense for open-science reforms to be supported by researchers who do stronger work (and there is evidence from betting markets that experts can predict reproducibility with some accuracy [67]) and opposed by those whose work has failed to replicate (for example, [225]). This would lead to open-science practices themselves being a marker of research quality. On the other hand, honesty and transparency are not enough [83]: openness and preregistration alone won’t endow replicability to a psychology study with a high ratio of noise to signal, which can happen when designs focus on procedural issues (e.g., randomization), to the detriment of theory and measurement.

Steps can be taken to reduce rhetorical risks. For example, Deyzer et al. [62] propose accompanying colloquial statements about reproducibility problems and solutions with formal problem statements and results, and provide questions to guide researchers in doing so. Greater rigor in reform arguments can mean quicker identification of logical errors, misinterpretations of constructs, or other blind spots in attempts to steer a field back on track.

6 ACKNOWLEDGMENTS

We thank Jake Hofman, Cyriel Zhang, Jean Czerlinski Oretge for comments. Hullman is supported by the NSF (IIS-1930642) and a Microsoft Faculty Fellowship, Narayanan by the NSF (IIS-1763642), and Gelman by the ONR.