What You See is What You Get: Distributional Generalization for Algorithm Design in Deep Learning

Anonymous Author(s)
Affiliation
Address
email

Abstract

We investigate and leverage a connection between Differential Privacy (DP) and the recently proposed notion of Distributional Generalization (DG). Applying this connection, we introduce new conceptual tools for designing deep-learning methods that bypass "pathologies" of standard stochastic gradient descent (SGD). First, we prove that differentially private methods satisfy a "What You See Is What You Get (WYSIWYG)" generalization guarantee: whatever a model does on its train data is almost exactly what it will do at test time. This guarantee is formally captured by distributional generalization. WYSIWYG enables principled algorithm design in deep learning by reducing *generalization* concerns to *optimization* ones: in order to mitigate unwanted behavior at test time, it is provably sufficient to mitigate this behavior on the train data. This is notably false for standard (non-DP) methods, hence this observation has applications even when privacy is not required. For example, importance sampling is known to fail for standard SGD, but we show that it has exactly the intended effect for DP-trained models. We use these insights to construct simple algorithms which match or outperform SOTA in several distributional robustness applications, and to significantly improve the privacy vs. disparate impact tradeoff of DP-SGD. Finally, we also improve on known theoretical bounds relating DP, stability, and distributional generalization.

1 Introduction

Much of machine learning (ML), both in theory and in practice, operates under two assumptions. First, we have i.i.d. samples from a distribution. Second, we care only about a single averaged scalar (e.g. error/loss/risk) over this distribution. Under these assumptions, we have mature methods and theory: Modern learning methods excel when trained on i.i.d. data to directly optimize a scalar loss, and there are many theoretical for reasoning about *generalization* which explain when does optimization of a scalar on the train dataset translates to similar values of this scalar at test time.

However, the focus on scalar metrics such as average error misses many theoretically, practically, and socially relevant aspects of model performance. For example, models with small *average* error often have high error on salient minority subgroups [Buolamwini and Gebru, 2018, Koenecke et al., 2020]. In general, ML models are applied to the heterogeneous and long-tailed data distributions of the real world [Van Horn and Perona, 2017]. Attempting to summarize their complex behavior with only a single scalar misses many rich and important aspects of learning.

These issues are compounded for modern overparameterized networks, as their nuanced test-time behavior is not reflected by their train sets. This presents an obstacle for algorithm design, because interventions which alter a network's properties on its train set do not always transfer to the test

Submitted to 36th Conference on Neural Information Processing Systems (NeurIPS 2022). Do not distribute.

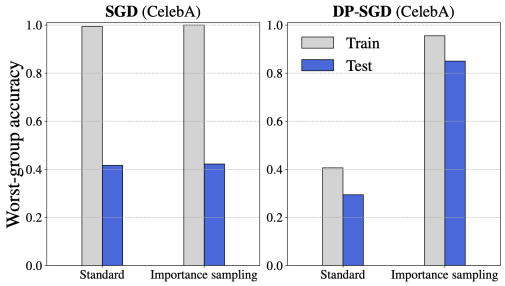


Figure 1: **Differential privacy ensures the desired behavior of importance sampling on test data.** The train and test accuracy of ResNets on CelebA, evaluated on the worst-performing ("male, blond") subgroup. *Left:* Standard SGD has a large generalization gap on this subgroup, and Importance Sampling (IS) has little effect. *Right:* DP-SGD provably has small generalization gap on all subgroups, and IS improves subgroup performance as intended. See Section 5 for details.

set. For example, consider the setting of *importance sampling*: suppose we know that a certain subgroup of inputs is underrepresented in the train dataset compared to the test distribution (breaking the "i.i.d. train/test" assumption). For underparameterized models, we can simply up-sample this underrepresented group to account for the distribution shift [see, e.g., Gretton et al., 2009]. This approach, however, is known to empirically fail for overparameterized models [Byrd and Lipton, 2019]. Because "what you see" (on the train dataset) is not "what you get" (at test time), we cannot make principled train-time interventions to affect test-time behaviors. This issue extends beyond importance sampling: for example, theoretically principled methods for distributionally robust optimization (e.g. Namkoong and Duchi [2016]) fail for overparameterized deep networks, and require ad-hoc modifications [Sagawa et al., 2019].

We develop a theoretical framework which (1) sheds light on these existing issues, and (2) leads to improved practical methods in privacy, fairness, and distributional robustness. The core object in our framework is what we call the "What You See Is What You Get" (WYSIWYG) property. A training procedure with the WYSIWYG property does *not* exhibit the pathologies of standard stochastic gradient descent (SGD): all test-time behaviors will be expressed on the train dataset as well, and there will be "no surprises" in generalization.

What You See Is What You Get (WYSIWYG) as a Design Principle. The WYSIWYG property is desirable for two reasons. The first is diagnostic: as there are "no surprises" at test time, all properties of a model at test time are already evident on the train dataset. It cannot be the case, for example, that a WYSIWYG model has small disparate impact on the train dataset, but large disparate impact at test time. The second reason is algorithmic: to mitigate *any* unwanted test-time behavior, it is sufficient to mitigate this behavior on the train dataset. This means that algorithm designers can be concerned only with achieving "good behavior" on the train dataset, and the WYSIWYG property guarantees good behavior at test time. In practice, this enables the usage of many theoretically principled algorithms which were developed in the underparameterized regime to also apply in the modern overparameterized (deep learning) setting. For example, we find that interventions such as importance sampling, or algorithms for distributionally robust optimization, which fail without additional regularization, work exactly as intended with WYSIWYG (See Figure 1 for an illustration).

As WYSIWYG is a high-level conceptual property, we have to formalize it to use in practice. We do so using the recent notion of *Distributional Generalization* (DG), as introduced by Nakkiran and Bansal [2020], Kulynych et al. [2022]. If classical generalization ensures that the values of the model's loss on the training dataset and at test time are close on average [Shalev-Shwartz et al., 2010], distributional generalization ensures that values of any other bounded test function (not only loss) are close on training and test time. We say that a model that satisfies an appropriate level of distributional generalization exhibits the WYSIWYG property.

Achieving DG via Differential Privacy (DP). Our key observation is that distributional generalization (DG) is formally implied by *differential privacy* (DP) [Dwork et al., 2006, 2014]). The spirit of this observation is not novel: DP training is known to satisfy much stronger notions of generalization (e.g., *robust generalization*, see Section 6 for more details), and stability than standard SGD [Dwork et al., 2015a, Cummings et al., 2016, Bassily et al., 2016]. We show that a similar connection holds for the notion of distributional generalization, and prove (and improve) tight bounds relating DP,

stability, and DG. In particular, we show that if a training procedure satisfies DP, it also satisfies DG. This guarantees the WYSIWYG property for any method that is differentially-private, including DP-SGD on deep neural networks [Abadi et al., 2016].

We demonstrate how DG can be a useful design principle in two concrete settings. First, we show that we can mitigate disparate impacts of DP training [Bagdasaryan et al., 2019, Pujol et al., 2020] by leveraging importance sampling. Second, we study the setting of distributionally robust optimization. We show how ideas from DP can be used to construct heuristic optimizers, which do not formally satisfy DP, yet empirically exhibit high DG. Our heuristics lead to competitive results with SOTA algorithms in five datasets in the distributional robustness setting.

Our Contributions. We develop the theoretical connection between Differential Privacy (DP) and Distributional Generalization (DG), and we leverage our theory to improve empirical performance in privacy, fairness, and robustness applications. Theoretically (Sections 2 to 4):

1. We provide tighter bounds than previously known connecting DP and strong forms of generalization, and show that DP training methods satisfy DG, thus the WYSIWYG property.
2. We introduce DP-IS-SGD, an importance-sampling version of DP-SGD, and show it satisfies DP and DG.

Experimentally (Section 5):

1. We use our framework to shed light on *disparate impact* of DP [Bagdasaryan et al., 2019]: The disparity in accuracy across groups at test time are provably reflected by the accuracy disparity *on the train dataset*.
2. We use our DP-IS-SGD algorithm to largely mitigate the disparate impact of DP using importance sampling.
3. Based on our theoretical intuitions, we propose a DP-inspired heuristic: addition of gradient noise. We find this empirically achieves competitive and even improved results in several DRO settings.

Taken together, our results emphasize the central role of distributional generalization—and the WYSIWYG property it implies—in designing machine learning algorithms which avoid the "pathologies" of standard SGD. We also establish DP as a useful tool for achieving DG, and thus extend its applications further beyond privacy.

2 Theory of "What You See is What You Get" Generalization

We first review the notion of distributional generalization and demonstrate why it implies the WYSIWYG property. Second, we show that stability implies distributional generalization. Finally, we improve on the known stability guarantees of differential privacy. As a result, we extend the connections between differential privacy, stability, and generalization to *distributional* generalization, showing that stability and privacy imply the WYSIWYG property.

Notation. We consider a learning task with a set of examples $\mathbb{X}$ and labels $\mathbb{Y}$. We assume that a *source distribution* of labeled examples $z \triangleq (x, y) \sim \mathcal{D}$ is defined over $\mathbb{D} = \mathbb{X} \times \mathbb{Y}$. Given an i.i.d.-sampled *dataset* $S \sim \mathcal{D}^n$ of size n, we use a randomized *training algorithm* $\theta(S)$ that outputs a model's parameter vector θ from the set Θ. We denote by $f_\theta(x)$ the resulting prediction function.

2.1 Distributional Generalization and WYSIWYG

If on-average generalization [Shalev-Shwartz et al., 2010] guarantees closeness only of loss values on train and test data, distributional generalization (DG) also guarantees closeness of values of all test functions $\phi(z; \theta) \in [0, 1]$ beyond only loss:

Definition 2.1 (Based on Nakkiran and Bansal [2020])**.** An algorithm $\theta(S)$ satisfies δ-distributional generalization if for all $\phi : \mathbb{D} \times \Theta \to [0, 1]$,

$$\left| \mathop{\mathbb{E}}_{\substack{S \sim \mathcal{D}^n \\ z \sim S}} \phi\big(z; \theta(S)\big) - \mathop{\mathbb{E}}_{\substack{S \sim \mathcal{D}^n \\ z \sim \mathcal{D}}} \phi\big(z; \theta(S)\big) \right| \leq \delta. \tag{1}$$

By the variational characterization of the total-variation distance, Equation (1) is equivalent to the bound $d_{\mathsf{TV}}(P_1, P_0) \leq \delta$, where P_1 and P_0 are both distributions of $\big(z, \theta(S)\big)$ over the randomness of $S \sim \mathcal{D}^n$ and the training algorithm $\theta(\cdot)$, with the difference that $z \sim S$ in the case of P_1 (train distribution), and $z \sim \mathcal{D}$ in the case of P_0 (test distribution).

It might seem that DG only ensures average closeness of bounded tests on train and test data. This is not, however, the full picture. Consider generalization in terms of a broader class of functions:

Definition 2.2 (Kulynych et al. [2022])**.** An algorithm $\theta(S)$ satisfies (δ, π)-distributional generalization if for a given property function $\pi : \mathbb{D} \times \Theta \to \mathbb{R}^k$ it holds that $d_{\mathsf{TV}}(\pi\sharp P_1, \pi\sharp P_0) \leq \delta$, where $\pi\sharp P$ is the distribution of $\pi(Z)$ for $Z \sim P$.

Because TV distance is preserved under post-processing, we can see that δ-distributional generalization implies (δ, π)-distributional generalization for *all* property functions. Informally, δ-DG means that for *all* numeric property functions $\pi(z; \theta)$ of a model, the distributions of the property values are close on the train and test data, on average. This fact captures the high-level idea of the *"What You See is What You Get"* (WYSIWYG) guarantee. Some example property functions:

- *Subgroup loss:* $\pi(z; \theta) = \mathbb{1}\{z \in G\} \cdot \ell(z; \theta)$, for some subgroup $G \subset \mathbb{D}$.
- *Counterfactual fairness:* $\pi((x, y); \theta) = f_\theta(\mathrm{CF}(x)) - f_\theta(x)$, where $\mathrm{CF}(x)$ is a counterfactual version of x had it had a different value of a sensitive attribute [Kusner et al., 2017].
- *Robustness to corruptions:* $\pi(z; \theta) = \ell(A(z); \theta)$, where $A(x)$ is a possibly randomized transformation that distorts the example, e.g., by adding Gaussian noise.
- *Adversarial robustness:* $\pi(z; \theta) = \ell(A_\theta(z); \theta)$, where $A_\theta(z)$ is an adversarial example, e.g. generated using the PGD attack [Madry et al., 2018].

In the next sections, we show how a training algorithm can provably satisfy DG and therefore provide WYSIWYG guarantees for all properties, including the ones above.

2.2 Distributional Generalization from Stability and Differential Privacy

The connections between privacy, stability, and generalization are well-known. In particular, stability of the learning algorithm—its non-sensitivity to limited changes in the training data—implies generalization [Bousquet and Elisseeff, 2002, Shalev-Shwartz et al., 2010]. In turn, differential privacy implies strong forms of stability, thus ensuring generalization through the chain Privacy $\Rightarrow$ Stability $\Rightarrow$ Generalization [Raskhodnikova et al., 2008, Dwork et al., 2015b,a, Wang et al., 2016].

Let us formally define differential privacy:

Definition 2.3 (Differential Privacy [Dwork et al., 2006, 2014])**.** An algorithm $\theta(S)$ is (ϵ, δ)-differentially private (DP) if for any two *neighbouring datasets*—differing by one example—S, S' of size n, for any subset $K \subseteq \Theta$ it holds that $\Pr[\theta(S) \in K] \leq \exp(\epsilon) \Pr[\theta(S') \in K] + \delta$.

DP mathematically encodes a notion of plausible deniability of the inclusion of an example in the dataset. However, it can also be thought as a strong form of stability [Dwork et al., 2015b]. As such, DP implies other notions of stability.

We consider the following notion, which has been studied in the literature under multiple names and contexts. In the context of privacy, it is equivalent to $(0, \delta)$-differential privacy, and has been called additive differential privacy [Geng et al., 2019], and total-variation privacy [Duchi et al., 2013]. In the context of learning, it has been called total-variation (TV) stability [Bassily et al., 2016]. We take this last approach and refer to it as TV stability:

Definition 2.4 (TV Stability)**.** An algorithm $\theta(S)$ is δ-TV stable if for any two *neighbouring datasets* S, S' of size n, for any subset $T \subseteq \Theta$ it holds that $\Pr[\theta(S) \in K] \leq \Pr[\theta(S') \in K] + \delta$.

It is easy to see that (ϵ, δ)-DP immediately implies $(\exp(\epsilon) - 1 + \delta)$-TV stability.

From Classical to Distributional Generalization. Similarly to the classical generalization, one way to achieve distributional generalization is through strong stability:

Theorem 2.5. *Suppose that the training algorithm is δ-TV stable. Then, the algorithm satisfies δ-DG.*

We refer to Appendix B for the proofs of this and all other formal statements in the rest of the paper.

As DP implies TV-stability, by Theorem 2.5 we have that DP also implies DG. Next, we show that DP algorithms enjoy a significantly stronger stability guarantee than the previously known one, which means that the DG guarantee that one obtains from DP is also stronger.

Proposition 2.6. *Suppose that the training algorithm is (ϵ, δ)-DP. Then, the algorithm satisfies δ'-TV stability with* $\delta' = \frac{\exp(\epsilon)-1+2\delta}{\exp(\epsilon)+1}$.

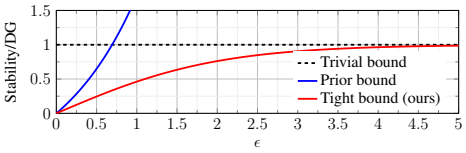


Figure 2: Bound on TV stability (therefore DG) from DP, assuming $\delta = 0$. x axis: ϵ level of DP. y axis: δ-level of TV stability/DG.

Figure 2 shows that the known bound of $\exp(\epsilon) + 1 - \delta$ quickly becomes vacuous, unlike ours. Moreover, in Appendix B we show that this bound is tight.

Stronger Distributional Generalization Guarantees. Although DG implies generalization bounds for all properties in a black-box way, it is sometimes possible to obtain tighter bounds for specific properties. For example, if we are concerned with accuracy on subgroups, then directly applying δ-DG to the *subgroup loss* property yields a bound that decays with the size of the subgroup: accuracy on very small subgroups is not guaranteed to generalize well. In Appendix C.1 we show that TV stability in fact implies "subgroup DG", which guarantees that the accuracy on even arbitrarily small subgroups generalizes well in expectation. As another example, in Appendix C.2 we show that TV stability also ensures the generalization of calibration properties of the learning algorithm.

3 Example Applications

To demonstrate that DG is a useful property in algorithm design, in the remainder of this paper we use it to construct simple and high-performing algorithms for two example applications: mitigation of disparate impact of DP and ensuring group-distributional robustness.

Mitigating Disparate Impact of DP. First, we consider applications in which learning presents privacy concerns, e.g., in the case that the training data contains sensitive information. Using training procedures that satisfy DP is a standard way to guarantee privacy in such settings. Training with DP, however, is known to incur *disparate impact* on the model accuracy: some subgroups of inputs can have worse test accuracy than others. For example, Bagdasaryan et al. [2019] show that using DP-SGD—a standard algorithm for satisfying DP [Abadi et al., 2016]—in place of regular SGD causes a significant accuracy drop on "darker skin" faces in models trained on the CelebA dataset of celebrity faces [Liu et al., 2015], but a less severe drop on "lighter skin" faces. Our goal is to mitigate such disparate impact. This issue—a quality-of-service harm [Madaio et al., 2020]—is but one of many possible harms due to ML systems. We do not aim to mitigate any other fairness-related issues, nor claim this is possible within our framework, or with technical solutions in general.

Formally, we assume the data distribution $\mathcal{D}$ is a mixture of m groups indexed by set $\mathcal{G} = \{1, \ldots, m\}$, such that $\mathcal{D} = \sum_{i=1}^{m} q_i \mathcal{D}_i$. The vector $(q_i, \ldots, q_m) \in [0, 1]^m$ represents the group probabilities, with $\sum_{i=1}^{m} q_i = 1$. For given parameters (ϵ, δ), we want to learn a model θ that simultaneously satisfies (ϵ, δ)-DP, has high overall accuracy, and incurs small *loss disparity*:

$$\max_{g,g' \in \mathcal{G}} \left| \mathop{\mathbb{E}}_{z \sim \mathcal{D}_g} [\ell(z; \theta)] - \mathop{\mathbb{E}}_{z \sim \mathcal{D}_{g'}} [\ell(z; \theta)] \right| . \tag{2}$$

Group-Distributional Robustness. Next, we consider a setting of *group-distributionally robust optimization* [e.g., Sagawa et al., 2019, Hu et al., 2018]. If in the standard learning approach we want to train a model that minimizes *average* loss, in this setting, we want to minimize the *worst-case (highest) group loss*. This objective can be used to mitigate fairness concerns such as those discussed previously, as well as to avoid learning spurious correlations [Sagawa et al., 2019].

Formally, we want to learn a model θ that minimizes the *worst-case group loss*:

$$\max_{g \in \mathcal{G}} \mathop{\mathbb{E}}_{z \sim \mathcal{D}_g} [\ell(z; \theta)] . \tag{3}$$

Unlike the previous application, in this setting, we do not require privacy of the training data. We use training with DP as a *tool* to ensure the generalization of the worst-case group loss, as described next.

Algorithm 1 DP-IS-SGD (DP Importance Sampling SGD)

Input: Training dataset S, model f_θ parameterized by θ, loss function ℓ; max gradient norm C, noise parameter σ, number of epochs T, sampling rate $\bar{p}$; group probabilities $\vec{q} = (q_1, \ldots, q_m)$

Output: θ_T

for $t = 1, \ldots, T$ **do**
  $\mathsf{Batch}_t \leftarrow \mathsf{Sample}_{p(\cdot)}(S)$, with $p(z) \triangleq \bar{p}/_{m \cdot q_{g(z)}}$
  $\Delta_t\theta \leftarrow 0$
  for $(x_i, y_i) \in \mathsf{Batch}_t$ **do**
    $\Delta_t\theta \leftarrow \Delta_t\theta + \mathsf{Clip}(\nabla_\theta \ell(f_\theta(x_i), y_i), C)$
  end for
  Sample $\xi_t \sim \sigma C \cdot \mathcal{N}(0, I_{d\times d})$
  $\Delta_t\theta \leftarrow \frac{1}{|\mathsf{Batch}_t|}\Delta_t\theta + \xi_t$
  $\theta_t \leftarrow \mathsf{Optimizer}(\theta_{t-1}, \Delta_t\theta)$
end for

The highlighted parts indicate the differences with respect to DP-SGD. We obtain DP-SGD as a special case when we have a single group with $q = 1$ (implying $p(z) = \bar{p}$).

4 Algorithms which Distributionally Generalize

In this section, we construct algorithms for the applications in Section 3. Our approach follows the blueprint: First, we apply a principled algorithmic intervention that ensures desired behavior on *the training dataset* (e.g., importance sampling). Second, we modify the resulting algorithm to additionally ensure DG, which guarantees that the desired behavior generalizes to the *test data*.

4.1 DP Training with Importance Sampling

Our first algorithm, DP-IS-SGD (Algorithm 1), is a version of DP-SGD [Abadi et al., 2016] which performs importance sampling. DP-IS-SGD is designed to mitigate disparate impact while retaining DP guarantees. The standard DP-SGD samples data batches using *uniform Poisson subsampling:* Each example in the training set is chosen into the batch according to the outcome of a Bernoulli trial with probability $\bar{p} \in [0, 1]$. To correct for unequal representation and the resulting disparate impact, we use *non-uniform Poisson subsampling*: Each example $z \in S$ has a possibly different probability $p(z)$ of being selected into the batch, where $p(z)$ does not depend on the dataset S otherwise, and is bounded: $0 \leq p(z) \leq p^* \leq 1$. We denote this subsampling procedure as $\mathsf{Sample}_{p(\cdot)}(S)$.

We assume that we know to which group any $z = (x, y)$ belongs, denoted as $g(z)$, e.g., the group is one of the features in x. We choose $p(z)$ to satisfy two properties. First, to increase the sampling probability for examples in minority groups: $p(z) \propto {}^1/_{q_{g(z)}}$. Second, to keep the average batch size equal to $\bar{p} \cdot n$ as in standard DP-SGD. In the rest of the paper, we assume that the group probabilities $(q_1, \ldots, q_m)$ are known, but it is possible to estimate them in a private way using standard methods [Nelson and Reuben, 2019]. We present DP-IS-SGD in Algorithm 1, along with its differences to the standard DP-SGD.

DP Properties of DP-IS-SGD. Uniform Poisson subsampling is well-known to amplify the privacy guarantees of an algorithm [Chaudhuri and Mishra, 2006, Li et al., 2012]. For example, Li et al. [2012] show that if an algorithm $\theta(S)$ satisfies (ϵ, δ)-DP, then $\theta \circ \mathsf{Sample}_{\bar{p}}(S)$ provides approximately $(O(\bar{p}\epsilon), \bar{p}\delta)$-DP for small values of ϵ. We show in Appendix B that non-uniform Poisson subsampling provides the same amplification guarantee with $\bar{p} = p^*$, where p^* is the maximum value of $p(\cdot)$.

As this guarantee is independent of the internal workings of $\theta(S)$, it is loose. For DP-SGD, one way of computing tight privacy guarantees of subsampling is using the notion of *Gaussian differential privacy* (GDP) [Dong et al., 2019]. GDP is parameterized by a single parameter μ. If an algorithm $\theta(S)$ satisfies μ-GDP, one can efficiently compute a set of (ϵ, δ)-DP guarantees also satisfied by $\theta(S)$ [Dong et al., 2019]. We show that we can use any GDP-based mechanism for computing the privacy guarantee of DP-SGD to obtain the privacy guarantees of DP-IS-SGD in a black-box manner:

Proposition 4.1. *Let us denote by $\mu(\bar{p}, \sigma, C, T)$ (see Algorithm 1) a function that returns a μ-GDP guarantee of DP-SGD. Then, DP-IS-SGD satisfies a GDP guarantee $\mu(p^*, \sigma, C, T)$.*

4.2 Group-DRO with Noisy Gradients

We showed that DP-IS-SGD enjoys theoretical guarantees for both DP and DG. However, DP models often have lower test accuracy compared to standard training [Chaudhuri et al., 2011]. This can be an unnecessary disadvantage in settings where privacy is not required, such as in group-distributional robustness. Thus, we explore non-DP algorithms which do not come with theoretical guarantees on DG, but are inspired by our theory, and satisfy good empirical DG in practice.

DP-SGD uses gradient clipping (line 5 in Algorithm 1) and gradient noise (lines 7–8). Individually, these are used as *regularization methods* for improving stability and generalization [Hardt et al., 2016, Neelakantan et al., 2015], thus possibly improving DG in practice. Following this, we relax DP-IS-SGD to only use addition of noise to the gradient as a regularizer. This sacrifices privacy in exchange for practical performance. Specifically, we apply *gradient noise* to three standard algorithms for achieving group-distributional robustness: importance sampling (IS-SGD), importance weighting (IW-SGD) [Gretton et al., 2009], and gDRO [Sagawa et al., 2019]. This results in the following variations: IS-SGD with noisy gradient (IS-SGD-n), IW-SGD with noisy gradient (IW-SGD-n), and gDRO with noisy gradient (gDRO-n). See Appendix D for more details.

5 Experiments

We empirically study the distributional generalization in real-world applications. The code for the experiments is available in the supplementary material.

Datasets. We consider five datasets, studied in the distributional robustness and fairness literature: CelebA [Liu et al., 2015], UTKFace [Zhang et al., 2017], iNaturalist2017 (iNat) [Horn et al., 2018], CivilComments [Borkan et al., 2019], and MultiNLI [Williams et al., 2018, Sagawa et al., 2019]. For every dataset, each example belongs to one group (e.g., CelebA) or multiple groups (e.g., CivilComments). For example, in the CelebA dataset, there are four groups: "blond male", "male with other hair color", "blond female", and "female with other hair color". We present more details on the datasets, their groups, and used model architectures in Appendix E.

5.1 Enforcing DG in Practice

We empirically confirm that a training procedure with DP guarantees also has a bounded DG gap.

In practice, it is not possible to compute the exact DG gap. As a proxy in the rest of the paper, we use the difference between train-time and test-time worst-group accuracy. This (1) follows the empirical approach by Nakkiran and Bansal [2020] which proposes to estimate the gap in Equation (1) using a finite set of test functions, and (2) measures the aspect of distributional generalization that is relevant to our applications. We provide more details on this choice of the proxy measure in Appendix E.2.

In Figure 3, we train a model on CelebA using DP-SGD for different levels of privacy ϵ. We see that the gap between training and testing worst-group accuracy increases as the level of privacy ε is weakened, which is consistent with our theoretical bounds.

In Appendix E.3 we also explore how regularization methods which do not formally imply DG, can empirically improve DG.

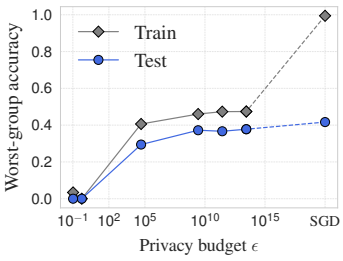
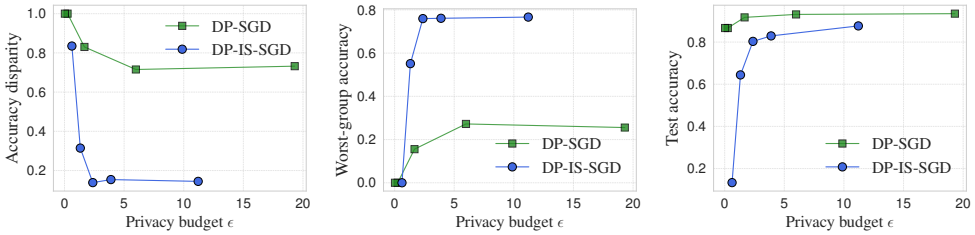


Figure 3: **Privacy induces DG.** Train/test worst-case group accuracies as a function of privacy parameter ϵ of DP-SGD on CelebA (x axis). Increasing privacy (left on x-axis) corresponds to a smaller generalization gap.

5.2 Disparate Impact of Differentially Private Models

We evaluate DP-IS-SGD (Algorithm 1), and demonstrate that it can mitigate the disparate impact in realistic settings where both privacy and fairness are required.

Figure 4 shows the accuracy disparity, test accuracy, and worst-case group accuracy, computed as in Equation (2), as a function of the privacy budget ϵ. The models are trained with DP-SGD and DP-IS-SGD. When comparing DP-SGD and DP-IS-SGD with the same or similar ϵ, we observe that DP-IS-SGD achieves lower disparity on all datasets. However, this comes with a drop in



(a) Accuracy disparity (lower is better) (b) Worst-group accuracy (higher is better) (c) Test accuracy (higher is better)

Figure 4: **Importance Sampling helps Disparate Impact of DP-SGD.** The accuracy disparity of the models trained with DP-SGD and DP-IS-SGD on CelebA. Adding importance sampling (IS) improves disparate impact at most privacy budgets in this setting. We set $\delta = 1/2n$, where n is the number of training examples. We use GDP accountant to compute the privacy budget ε.

average accuracy. On CelebA, for example, with $\epsilon \in [2, 12]$, DP-IS-SGD has around 8 p.p. lower test accuracy than DP-SGD. At the same time, the disparity drop ranges from 40 p.p. to 60 p.p., which is significantly higher than the accuracy drop. We observe similar results on UTKFace, as shown in Appendix E. On iNat, however, although DP-IS-SGD decreases disparity, the overall test accuracy suffers a significant hit. This is likely because the minority subgroup is extremely small, and importance-sampling are poorly behaved for very small groups. Details for UTKFace and iNat appear in Appendix E.

In summary, we find that DP-IS-SGD achieves lower disparity at the same privacy budget compared to standard DP-SGD, with only mild impact on test accuracy.

5.3 Group-DRO

We investigate whether our proposed versions of standard algorithms with Gaussian gradient noise (Section 4.2) can improve group-distributional robustness. We evaluate empirical DG using worst-group accuracy as a proxy for DG gap as in Section 5.1, following the evaluation criteria in prior work [Sagawa et al., 2019, Idrissi et al., 2021]. State-of-the-art (SOTA) methods apply ℓ_2 regularization and early-stopping to achieve the best performance. We compare three baselines with ℓ_2 regularization, IS-SGD-ℓ_2, IW-SGD-ℓ_2, and gDRO-ℓ_2 to our three noisy-gradient variations: IS-SGD-n, IW-SGD-n, and gDRO-n, as well as DP-IS-SGD. We use the validation set to select the best-performing regularization parameter and epoch (for early stopping) for each method. See Appendix E for details on the experimental setup.

Table 1 shows the worst-group accuracy of each algorithm on five datasets.[1] When comparing IS-SGD, IW-SGD, and gDRO with their noisy counterparts, we observe that the noisy versions in general have similar or slightly better performance compared to non-noisy counterparts. For instance, IS-SGD-n improves the SOTA results on CivilComments dataset. This showcases that in terms of learning distributionally robust models, *noisy gradient can be potentially a more effective regularizer than the currently standard ℓ_2 regularizer*.

We also find that DP-IS-SGD improves on baseline methods or even achieves similar SOTA performance on several datasets. For instance, on CelebA and MNLI, DP-IS-SGD achieves better performance than IS-SGD-ℓ_2, and achieves comparable performance to SOTA. This is surprising, as DP tends to deteriorate performance. This suggests that distributional robustness and privacy might not be incompatible goals. Moreover, DP can be a useful tool even when privacy is not required.

6 Related Work

DP and Strong Forms of Generalization. DP is known to imply a stronger than standard notion of generalization, called *robust generalization*[2] [Cummings et al., 2016, Bassily et al., 2016]. Robust

[1] IW-SGD numbers in Table 1 are different from Fig. 1, as in the figure we do not apply regularization.

[2] This term has also been recently used as a shorthand for "adversarially robust generalization", but robust generalization in the sense of Bassily et al. [2016] is a different and unrelated concept.

Table 1: The worst-group accuracy of each algorithm. gDRO-ℓ_2-SOTA shows the average and standard error over five runs from Idrissi et al. [2021]. Baselines are in the top rows; our algorithms are in the bottom. For CelebA, we show mean and standard error over three random splits. Our noisy gradient algorithms produce competitive results compared to their counterparts with ℓ_2 regularization.

	CelebA	UTKFace	iNat.	Civil.	MNLI
SGD-ℓ_2	73.0 ± 2.2	86.3	41.8	57.4	67.9
IS-SGD-ℓ_2	82.4 ± 0.5	85.8	70.6	64.3	70.4
IW-SGD-ℓ_2	$\mathbf{89.0} \pm 0.9$	86.5	67.6	65.7	68.1
gDRO-ℓ_2	84.5 ± 0.8	85.2	67.3	67.3	75.9
gDRO-ℓ_2-SOTA	86.9 ± 0.5	—	—	69.9 ± 0.5	$\mathbf{78.0} \pm 0.3$
DP-IS-SGD	86.0 ± 0.8	82.5	51.4	70.4	72.3
IS-SGD-n	84.9 ± 1.0	85.5	**71.0**	**71.9**	70.8
IW-SGD-n	$\mathbf{88.5} \pm 0.4$	**88.5**	70.9	69.9	69.7
gDRO-n	83.3 ± 0.5	87.5	56.4	71.3	**78.0**

generalization can be thought as a high-probability counterpart of DG: generalization holds with high probability over the train dataset, not only on average over datasets. In particular, it is possible to recover our result that DP implies DG as a consequence of these prior works, although with loose bounds. We focus on our notion of DG for both conceptual and theoretical simplicity: DG formulated as in Equation (1) enables us to prove tight theoretical bounds that are independent of sample size. A more comprehensive discussion of relations to robust generalization is in Appendix A. It can also be useful to consider intermediary definitions, varying in strength from DG to robust generalization. In Appendix C, we introduce such an notion ("strong DG") and show its connections to DP.

Disparate Impact of DP. Bagdasaryan et al. [2019], Pujol et al. [2020] have shown that ensuring DP in algorithmic systems can cause error disparity across population groups. Concurrently, Xu et al. [2021] have proposed DP-SGD-F, a variant of DP-SGD [Abadi et al., 2016] that dynamically adapts gradient-clipping bounds for different groups to reduce such disparate impact. We show that a simpler approach based on importance sampling is also an effective way to reduce disparities, and we provide a more general blueprint for designing algorithms with similar mitigations.

Group-Distributional Robustness. Group-distributional robustness aims to improve the worst-case group performance. Existing approaches include using worst-case group loss [Mohri et al., 2019, Sagawa et al., 2019, Zhang et al., 2020], balancing majority and minority groups by reweighting or subsampling [Byrd and Lipton, 2019, Sagawa et al., 2020, Idrissi et al., 2021], leveraging generative models [Goel et al., 2020], and applying various regularization techniques [Sagawa et al., 2019, Cao et al., 2019]. Although some work [Sagawa et al., 2019, Cao et al., 2019] discusses the importance of regularization in distributional robustness, they have not explored potential reasons for this importance (e.g. via the connection to distributional generalization). Another line of work studies how to improve group performance without group annotations [Duchi et al., 2021, Liu et al., 2021a, Creager et al., 2021], which is a different setting from ours as we assume the group annotations are known.

7 Conclusions

We argue that distributional generalization (DG) is a desirable property for learning algorithms, enabling more principled algorithm design in settings including deep learning. DG captures a high-level "What You See is What You Get" property, which ensures that *any* training-time behavior is reproduced at test time. We show that this property is possible to achieve, by proving it is implied by differential privacy. This enables us to leverage advances in differential privacy (such as DP-SGD for neural networks) to enforce DG in many applications.

We propose enforcing DG as a general design principle, and we use it to construct simple yet effective algorithms in two settings. In certain fairness settings, we largely mitigate the disparate impact of differential privacy by using importance sampling and enforcing DG in our new algorithm DP-IS-SGD. In certain distributional robustness settings, inspired by DP-SGD, we propose using a noisy gradient regularizer instead of the traditional ℓ_2 regularizer to enforce DG. Compared to SOTA algorithms, noisy gradient regularization can achieve competitive results across many standard benchmarks. We hope future work can explore extending this algorithmic design principle to other settings, such as adversarial robustness, counterfactual fairness, and calibration.

References

Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016.

Eugene Bagdasaryan, Omid Poursaeed, and Vitaly Shmatikov. Differential privacy has disparate impact on model accuracy. In *Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, December 8-14, 2019, Vancouver, BC, Canada*, 2019.

Raef Bassily, Kobbi Nissim, Adam D. Smith, Thomas Steinke, Uri Stemmer, and Jonathan R. Ullman. Algorithmic stability for adaptive data analysis. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, 2016.

Daniel Borkan, Lucas Dixon, Jeffrey Sorensen, Nithum Thain, and Lucy Vasserman. Nuanced metrics for measuring unintended bias with real data for text, classification. *arXiv preprint arXiv:1903.04561*, 2019.

Olivier Bousquet and André Elisseeff. Stability and generalization. *The Journal of Machine Learning Research*, 2, 2002.

Zhiqi Bu, Jinshuo Dong, Qi Long, and Weijie J Su. Deep learning with gaussian differential privacy. *Harvard data science review*, 2020(23), 2020.

Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*. PMLR, 2018.

Jonathon Byrd and Zachary Chase Lipton. What is the effect of importance weighting in deep learning? In *Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA*, volume 97 of *Proceedings of Machine Learning Research*, 2019.

Kaidi Cao, Colin Wei, Adrien Gaidon, Nikos Arechiga, and Tengyu Ma. Learning imbalanced datasets with label-distribution-aware margin loss. *Advances in Neural Information Processing Systems*, 32:1567–1578, 2019.

Kamalika Chaudhuri and Nina Mishra. When random sampling preserves privacy. In *Annual International Cryptology Conference*. Springer, 2006.

Kamalika Chaudhuri, Claire Monteleoni, and Anand D Sarwate. Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12(3), 2011.

Elliot Creager, Jörn-Henrik Jacobsen, and Richard Zemel. Environment inference for invariant learning. In *International Conference on Machine Learning*, pages 2189–2200. PMLR, 2021.

Rachel Cummings, Katrina Ligett, Kobbi Nissim, Aaron Roth, and Zhiwei Steven Wu. Adaptive learning with robust generalization guarantees. In *Proceedings of the 29th Conference on Learning Theory, COLT 2016, New York, USA, June 23-26, 2016*, volume 49 of *JMLR Workshop and Conference Proceedings*, 2016.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 2019.

Jinshuo Dong, Aaron Roth, and Weijie J Su. Gaussian differential privacy. *arXiv preprint arXiv:1905.02383*, 2019.

John C Duchi, Michael I Jordan, and Martin J Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, 2013.

John C Duchi, Peter W Glynn, and Hongseok Namkoong. Statistics of robust optimization: A generalized empirical likelihood approach. *Mathematics of Operations Research*, 2021.

Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*. Springer, 2006.

Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4), 2014.

Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Aaron Roth. Generalization in adaptive data analysis and holdout reuse. In *Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015, December 7-12, 2015, Montreal, Quebec, Canada*, 2015a.

Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Aaron Leon Roth. Preserving statistical validity in adaptive data analysis. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, 2015b.

Quan Geng, Wei Ding, Ruiqi Guo, and Sanjiv Kumar. Optimal noise-adding mechanism in additive differential privacy. In *The 22nd International Conference on Artificial Intelligence and Statistics, AISTATS 2019, 16-18 April 2019, Naha, Okinawa, Japan*, volume 89 of *Proceedings of Machine Learning Research*, 2019.

Karan Goel, Albert Gu, Yixuan Li, and Christopher Re. Model patching: Closing the subgroup performance gap with data augmentation. In *International Conference on Learning Representations*, 2020.

Arthur Gretton, Alex Smola, Jiayuan Huang, Marcel Schmittfull, Karsten Borgwardt, and Bernhard Schölkopf. Covariate shift by kernel mean matching. *Dataset shift in machine learning*, 3(4):5, 2009.

Moritz Hardt, Ben Recht, and Yoram Singer. Train faster, generalize better: Stability of stochastic gradient descent. In *Proceedings of the 33nd International Conference on Machine Learning, ICML 2016, New York City, NY, USA, June 19-24, 2016*, volume 48 of *JMLR Workshop and Conference Proceedings*, 2016.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016*, 2016.

Grant Van Horn, Oisin Mac Aodha, Yang Song, Yin Cui, Chen Sun, Alexander Shepard, Hartwig Adam, Pietro Perona, and Serge J. Belongie. The inaturalist species classification and detection dataset. In *2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018*, 2018.

Weihua Hu, Gang Niu, Issei Sato, and Masashi Sugiyama. Does distributionally robust supervised learning give robust classifiers? In *Proceedings of the 35th International Conference on Machine Learning, ICML 2018, Stockholmsmässan, Stockholm, Sweden, July 10-15, 2018*, volume 80 of *Proceedings of Machine Learning Research*, 2018.

Badr Youbi Idrissi, Martin Arjovsky, Mohammad Pezeshki, and David Lopez-Paz. Simple data balancing achieves competitive worst-group-accuracy. *arXiv preprint arXiv:2110.14503*, 2021.

Bargav Jayaraman and David Evans. Evaluating differentially private machine learning in practice. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1895–1912, 2019.

Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The composition theorem for differential privacy. In *Proceedings of the 32nd International Conference on Machine Learning, ICML 2015, Lille, France, 6-11 July 2015*, volume 37 of *JMLR Workshop and Conference Proceedings*, 2015.

Allison Koenecke, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R Rickford, Dan Jurafsky, and Sharad Goel. Racial disparities in automated speech recognition. *Proceedings of the National Academy of Sciences*, 117(14):7684–7689, 2020.

Pang Wei Koh, Shiori Sagawa, Henrik Marklund, Sang Michael Xie, Marvin Zhang, Akshay Balsubramani, Weihua Hu, Michihiro Yasunaga, Richard Lanas Phillips, Irena Gao, et al. Wilds: A benchmark of in-the-wild distribution shifts. In *International Conference on Machine Learning*. PMLR, 2021.

Bogdan Kulynych, Mohammad Yaghini, Giovanni Cherubin, Michael Veale, and Carmela Troncoso. Disparate vulnerability to membership inference attacks. *Proceedings on Privacy Enhancing Technologies*, 2022(1), 2022.

Matt J. Kusner, Joshua R. Loftus, Chris Russell, and Ricardo Silva. Counterfactual fairness. In *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, 2017.

Ninghui Li, Wahbeh Qardaji, and Dong Su. On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, 2012.

Evan Z Liu, Behzad Haghgoo, Annie S Chen, Aditi Raghunathan, Pang Wei Koh, Shiori Sagawa, Percy Liang, and Chelsea Finn. Just train twice: Improving group robustness without training group information. In *International Conference on Machine Learning*, pages 6781–6792. PMLR, 2021a.

Jiaxiang Liu, Simon Oya, and Florian Kerschbaum. Generalization techniques empirically outperform differential privacy against membership inference. *arXiv preprint arXiv:2110.05524*, 2021b.

Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. Deep learning face attributes in the wild. In *2015 IEEE International Conference on Computer Vision, ICCV 2015, Santiago, Chile, December 7-13, 2015*, 2015.

Ilya Loshchilov and Frank Hutter. Decoupled weight decay regularization. In *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*, 2019.

Michael A Madaio, Luke Stark, Jennifer Wortman Vaughan, and Hanna Wallach. Co-designing checklists to understand organizational challenges and opportunities around fairness in ai. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*, 2018.

Mehryar Mohri, Gary Sivek, and Ananda Theertha Suresh. Agnostic federated learning. In *International Conference on Machine Learning*, pages 4615–4625. PMLR, 2019.

Preetum Nakkiran and Yamini Bansal. Distributional generalization: A new kind of generalization. *arXiv preprint arXiv:2009.08092*, 2020.

Hongseok Namkoong and John C. Duchi. Stochastic gradient methods for distributionally robust optimization with f-divergences. In *Advances in Neural Information Processing Systems 29: Annual Conference on Neural Information Processing Systems 2016, December 5-10, 2016, Barcelona, Spain*, 2016.

Arvind Neelakantan, Luke Vilnis, Quoc V Le, Ilya Sutskever, Lukasz Kaiser, Karol Kurach, and James Martens. Adding gradient noise improves learning for very deep networks. *arXiv preprint arXiv:1511.06807*, 2015.

Boel Nelson and Jenni Reuben. Sok: Chasing accuracy and privacy, and catching both in differentially private histogram publication. *arXiv preprint arXiv:1910.14028*, 2019.

Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-performance deep learning library. *Advances in neural information processing systems*, 32: 8026–8037, 2019.

David Pujol, Ryan McKenna, Satya Kuppam, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Fair decision making using privacy-protected data. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, pages 189–199, 2020.

Sofya Raskhodnikova, Adam Smith, Homin K Lee, Kobbi Nissim, and Shiva Prasad Kasiviswanathan. What can we learn privately. In *Proceedings of the 54th Annual Symposium on Foundations of Computer Science*, 2008.

Shiori Sagawa, Pang Wei Koh, Tatsunori B Hashimoto, and Percy Liang. Distributionally robust neural networks for group shifts: On the importance of regularization for worst-case generalization. *arXiv preprint arXiv:1911.08731*, 2019.

Shiori Sagawa, Aditi Raghunathan, Pang Wei Koh, and Percy Liang. An investigation of why overparameterization exacerbates spurious correlations. In *International Conference on Machine Learning*, pages 8346–8356. PMLR, 2020.

Shai Shalev-Shwartz, Ohad Shamir, Nathan Srebro, and Karthik Sridharan. Learnability, stability and uniform convergence. *The Journal of Machine Learning Research*, 11, 2010.

Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, pages 3–18. IEEE, 2017.

Grant Van Horn and Pietro Perona. The devil is in the tails: Fine-grained classification in the wild. *arXiv preprint arXiv:1709.01450*, 2017.

Yu-Xiang Wang, Jing Lei, and Stephen E Fienberg. Learning with differential privacy: Stability, learnability and the sufficiency and necessity of erm principle. *The Journal of Machine Learning Research*, 17(1), 2016.

Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489), 2010.

Adina Williams, Nikita Nangia, and Samuel Bowman. A broad-coverage challenge corpus for sentence understanding through inference. In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers)*, 2018.

Thomas Wolf, Lysandre Debut, Victor Sanh, Julien Chaumond, Clement Delangue, Anthony Moi, Pierric Cistac, Tim Rault, Rémi Louf, Morgan Funtowicz, et al. Huggingface's transformers: State-of-the-art natural language processing. *arXiv preprint arXiv:1910.03771*, 2019.

Depeng Xu, Wei Du, and Xintao Wu. Removing disparate impact on model accuracy in differentially private stochastic gradient descent. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, pages 1924–1932, 2021.

Yao-Yuan Yang, Cyrus Rashtchian, Hongyang Zhang, Ruslan Salakhutdinov, and Kamalika Chaudhuri. A closer look at accuracy vs. robustness. In *Proceedings of Neural Information Processing Systems (NeurIPS)*, 2020.

Ashkan Yousefpour, Igor Shilov, Alexandre Sablayrolles, Davide Testuggine, Karthik Prasad, Mani Malek, John Nguyen, Sayan Ghosh, Akash Bharadwaj, Jessica Zhao, Graham Cormode, and Ilya Mironov. Opacus: User-friendly differential privacy library in PyTorch. *arXiv preprint arXiv:2109.12298*, 2021.

Jingzhao Zhang, Aditya Menon, Andreas Veit, Srinadh Bhojanapalli, Sanjiv Kumar, and Suvrit Sra. Coping with label shift via distributionally robust optimisation. *arXiv preprint arXiv:2010.12230*, 2020.

Zhifei Zhang, Yang Song, and Hairong Qi. Age progression/regression by conditional adversarial autoencoder. In *2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017*, 2017.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes]
   (b) Did you describe the limitations of your work? [Yes] We address the limitations where appropriate, e.g., high-level limitations in Section 3, and the fact that some methods we use in the empirical evaluations deviate from theory in Sections 4 and 5.
   (c) Did you discuss any potential negative societal impacts of your work? [Yes] In Section 3 we caution against using WYSIWYG for fairness-washing through technical solutionism. Other than this, our potential negative societal impacts are the same as with any other academic work which aims to improve the performance of deep learning: we risk improving performance of deep learning in downstream applications that are harmful, e.g., privacy-invasive, or violating other civil liberties. It is beyond the scope of our work to discuss such broad issues.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes]
   (b) Did you include complete proofs of all theoretical results? [Yes] See Appendix B.
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] We included the experiment code as supplemental material.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] See Appendix E.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [Yes] For experimental settings in which it was feasible for us to repeat experiments multiple times, we reported the standard errors (Table 1).
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] See Appendix E.1.
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] See Appendix E.1.
   (b) Did you mention the license of the assets? [Yes] See Appendix E.1.
   (c) Did you include any new assets either in the supplemental material or as a URL? [N/A]
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [Yes] See Appendix E.1.
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [Yes] See Appendix E.1.
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]