Incorporating Label Uncertainty in Understanding Adversarial Robustness

Xiao Zhang and David Evans
Department of Computer Science
University of Virginia
{shawn, evans}@virginia.edu

Abstract

A fundamental question in adversarial machine learning is whether a robust classifier exists for a given task. A line of research has made progress towards this goal by studying concentration of measure, but without considering data labels. We argue that the standard concentration fails to fully characterize the intrinsic robustness of a classification problem, since it ignores data labels which are essential to any classification task. Building on a novel definition of label uncertainty, we empirically demonstrate that error regions induced by state-of-the-art models tend to have much higher label uncertainty compared with randomly-selected subsets. This observation motivates us to adapt a concentration estimation algorithm to account for label uncertainty, resulting in more accurate intrinsic robustness measures for benchmark image classification problems. We further provide empirical evidence showing that adding an abstain option for classifiers based on label uncertainty can help improve both the clean and robust accuracies of models.

1 Introduction

Since the initial reports of adversarial examples against DNNs (Szegedy et al., 2014; Goodfellow et al., 2015), many defensive mechanisms have been proposed aiming to enhance the robustness of machine learning classifiers. Most have failed, however, against stronger adaptive attacks (Athalye et al., 2018; Tramer et al., 2020). PGD-based adversarial training (Madry et al., 2018) and its variants (Zhang et al., 2019; Carmon et al., 2019) are among the few heuristic defenses that have not been broken so far, but these methods still fail to produce satisfactorily robust classifiers, even for classification tasks on benchmark datasets like CIFAR-10. Motivated by the empirical hardness of adversarially-robust learning, a line of theoretical works (Gilmer et al., 2018; Fawzi et al., 2018; Mahloujifar et al., 2019a; Shafahi et al., 2019) have argued that adversarial examples are unavoidable. In particular, these works proved that as long as the input distributions are concentrated with respect to the perturbation metric, adversarially robust classifiers do not exist. Recently, Mahloujifar et al. (2019b) and Prescott et al. (2021) generalized these results by developing empirical methods for measuring the concentration of arbitrary input distribution that can be further translated into an intrinsic robustness limit. (Appendix A provides a more thorough discussion of related work.)

We argue that the standard concentration of measure problem, which was studied in all of the aforementioned works, is not sufficient to capture a realistic intrinsic robustness limit for a classification problem. In particular, the standard concentration function is defined as an inherent property regarding the input metric probability space, which does not take account of the underlying label information. We argue that such label information is an essential component for any supervised learning problem, including adversarially robust classification, so must be incorporated into intrinsic robustness limits.

Contributions. We identify the insufficiency of the standard concentration of measure problem and provide explanations on why it fails to capture a realistic intrinsic robustness limit (Section 3).
Then, we introduce the notion of label uncertainty (Definition 4.1), which characterizes the average uncertainty of label assignments for an input region. Building on this definition, we incorporate label uncertainty in the standard concentration measure as an initial step towards a more realistic characterization of intrinsic robustness (Section 4). Experiments on the CIFAR-10 and CIFAR-10H datasets (Peterson et al., 2019) demonstrate that error regions induced by state-of-the-art classification models all have high label uncertainty (Section 6.1), which validates the proposed label uncertainty constrained concentration problem.

By adapting the standard concentration estimation method in Mahloujifar et al. (2019b), we propose an empirical estimator for the label uncertainty constrained concentration function. We then theoretically study the asymptotic behavior of the proposed estimator and provide a corresponding heuristic algorithm for typical perturbation metrics (Section 5). Compared with existing methods based on standard concentration, we demonstrate that our method is able to produce a more accurate characterization of intrinsic robustness limit for benchmark datasets such as CIFAR-10 (Section 6.2). We also provide empirical evidence showing that both the clean and robust accuracies of state-of-the-art robust classification models are largely affected by the label uncertainty of the tested examples, suggesting that adding an abstain option based on label uncertainty is a promising avenue for improving adversarial robustness (Section 6.3).

Notation. We use lowercase boldface letters to denote vectors and use \([k]\) to denote \(\{1, 2, \ldots, k\}\). For any set \(A\), let \(|A|\), \(\text{pow}(A)\) and \(I_A(\cdot)\) be the cardinality, all measurable subsets and the indicator function of \(A\). Consider metric probability space \((X, \mu, \Delta)\), where \(\Delta : X \times X \to \mathbb{R}_{\geq 0}\) is a distance metric on \(X\). Define the empirical measure of \(\mu\) with respect to a data set \(S\) sampled from \(\mu\) as \(\hat{\mu}_S(A) = \sum_{x \in S} I_A(x) / |S|\). Denote by \(B_\epsilon^\Delta(x)\) the ball around \(x\) with radius \(\epsilon\) measured by \(\Delta\).

Define the \(\epsilon\)-expansion of \(A\) as \(A(\epsilon, \Delta) = \{x \in X : \exists \, x' \in B_\epsilon^\Delta(x) \cap A\}\). When \(\Delta\) is free of context, we simply write \(B_\epsilon(x) = B_\epsilon^\Delta(x)\) and \(A_\epsilon = A(\epsilon, \Delta)\). Denote by \(I_n\) the \(n \times n\) identity matrix.

2 Preliminaries

Adversarial Risk and Robustness. Adversarial risk captures the vulnerability of a classifier against adversarial perturbations. In particular, we work with the following adversarial risk definition, which has been studied in several previous works, such as [Gilmer et al., 2018; Bubeck et al. (2019); Mahloujifar et al. (2019a,b); Zhang et al. (2020b); Prescott et al. (2021)].

Definition 2.1 (Adversarial Risk). Let \((X, \mu, \Delta)\) be a metric probability space of instances and \(Y\) be the set of possible class labels. Assume \(c : X \to Y\) is a concept function that gives each instance a label. For any classifier \(f : X \to Y\) and \(\epsilon \geq 0\), the adversarial risk of \(f\) is defined as:

\[
\text{AdvRisk}_\epsilon(f, c) = \Pr_{x \sim \mu} \left[ \exists x' \in B_\epsilon(x) \text{ s.t. } f(x') \neq c(x') \right].
\]

The adversarial robustness of \(f\) is defined as: \(\text{AdvRob}_\epsilon(f, c) = 1 - \text{AdvRisk}_\epsilon(f, c)\).

When \(\epsilon = 0\), adversarial risk equals to the standard risk. Namely, \(\text{AdvRisk}_0(f, c) = \text{Risk}(f, c) := \Pr_{x \sim \mu}[f(x) \neq c(x)]\) holds for any classifier \(f\). Other definitions of adversarial risk have been proposed, such as the one used in [Madry et al., 2018]. These definitions are equivalent the one we use, as long as small perturbations preserve the labels assigned by \(c(\cdot)\).

Intrinsic Robustness. The definition of intrinsic robustness was first introduced by Mahloujifar et al. (2019b) to capture the maximum adversarial robustness with respect to some set of classifiers:

Definition 2.2 (Intrinsic Robustness). Consider the input metric probability space \((X, \mu, \Delta)\) and the set of labels \(Y\). Let \(c : X \to Y\) be a concept function that gives a label to each input. For any set of classifiers \(F \subseteq \{f : X \to Y\}\) and \(\epsilon \geq 0\), the intrinsic robustness with respect to \(F\) is defined as:

\[
\text{AdvRob}_\epsilon(F, c) = 1 - \inf_{f \in F} \{ \text{AdvRisk}_\epsilon(f, c) \} = \sup_{f \in F} \{ \text{AdvRob}_\epsilon(f, c) \}.
\]

According to the definition of intrinsic robustness, there does not exist any classifier in \(F\) with adversarial robustness higher than \(\text{AdvRob}_\epsilon(F, c)\) for the considered task. Prior works, including [Gilmer et al., 2018; Mahloujifar et al. (2019a,b); Zhang et al. (2020b)], selected \(F\) in Definition 2.2 as the set of imperfect classifiers \(F_\alpha = \{ f : \text{Risk}(f, c) \geq \alpha \}\), where \(\alpha \in (0, 1)\) is some constant.
Concentration of Measure. Concentration of measure captures a ‘closeness’ property for a metric probability space of instances. More formally, it is defined by the concentration function:

**Definition 2.3 (Concentration Function).** Let $(\mathcal{X}, \mu, \Delta)$ be a metric probability space. For any $\alpha \in (0, 1)$ and $\epsilon \geq 0$, the concentration function of $(\mathcal{X}, \mu, \Delta)$ is defined as:

$$h(\mu, \alpha, \epsilon) = \inf_{\mathcal{E} \in \text{pow}(\mathcal{X})} \{ \mu(\mathcal{E}) : \mu(\mathcal{E}) \geq \alpha \}.$$

The standard notion of concentration function considers a special case of Definition 2.3 with $\alpha = 1/2$ (e.g., Talagrand (1995)). For some special metric probability spaces, one can prove the closed-form solution of the concentration function. The Gaussian Isoperimetric Inequality (Borell, 1975; Sudakov & Tsirelson, 1974) characterizes the concentration function for spherical Gaussian distribution and $\ell_2$-norm distance metric, and was generalized by Prescott et al. (2021) to other $\ell_p$ norms.

3 Standard Concentration is Insufficient

We first explain a fundamental connection between the concentration of measure and the intrinsic robustness with respect to imperfect classifiers shown in previous work, and then argue that standard concentration fails to capture a realistic intrinsic robustness limit because it ignores data labels.

**Connecting Intrinsic Robustness with Concentration of Measure.** Let $(\mathcal{X}, \mu, \Delta)$ be the considered input metric probability space, $\mathcal{Y}$ be the set of possible labels, and $c : \mathcal{X} \to \mathcal{Y}$ be the concept function that gives each input a label. Given parameters $0 < \alpha < 1$ and $\epsilon \geq 0$, the standard concentration problem can be cast into an optimization problem as follows:

$$\min_{\mathcal{E} \in \text{pow}(\mathcal{X})} \mu(\mathcal{E}) \quad \text{subject to} \quad \mu(\mathcal{E}) \geq \alpha. \quad (3.1)$$

For any classifier $f$, let $\mathcal{E}_f = \{ x \in \mathcal{X} : f(x) \neq c(x) \}$ be its induced error region with respect to $c(\cdot)$. By connecting the risk of $f$ with the measure of $\mathcal{E}_f$ and the adversarial risk of $f$ with the measure of the $\epsilon$-expansion of $\mathcal{E}_f$, Mahloujifar et al. (2019a) proved that the standard concentration problem (3.1) is equivalent to the following optimization problem regarding risk and adversarial risk:

$$\min_f \text{AdvRisk}_\epsilon(f, c) \quad \text{subject to} \quad \text{Risk}(f, c) \geq \alpha.$$ 

More specifically, the following lemma characterizes the fundamental connection between the concentration function and the intrinsic robustness with respect to the set of imperfect classifiers:

**Lemma 3.1 (Mahloujifar et al., 2019a).** Let $\alpha \in (0, 1)$ and $\mathcal{F}_\alpha = \{ f : \text{Risk}(f, c) \geq \alpha \}$ be the set of imperfect classifiers. For any $\epsilon \geq 0$, it holds that

$$\text{AdvRob}_\epsilon(\mathcal{F}_\alpha, c) = 1 - h(\mu, \alpha, \epsilon).$$

Lemma 3.1 suggests that the concentration function of the input metric probability space $h(\mu, \alpha, \epsilon)$ can be translated into an adversarial robustness upper bound that applies to any classifier with risk at least $\alpha$. If this upper bound is shown to be small, then one can conclude that it is impossible to learn an adversarially robust classifier, as long as the learned classifier has risk at least $\alpha$.

**Concentration without Labels Mischaracterizes Intrinsic Robustness.** Despite the appealing relationship between concentration of measure and intrinsic robustness, we argue that solving the standard concentration problem is not enough to capture a meaningful intrinsic limit for adversarially robust classification. Recall that the standard concentration of measure problem (3.1) aims to find the optimal subset that has the smallest $\epsilon$-expansion with regard to the input metric probability space $(\mathcal{X}, \mu, \Delta)$; the underlying concept function $c(\cdot)$ that determines the underlying class label of each input is not involved. For the considered metric probability space, no matter how we assign the labels to the inputs, the concentration function $h(\mu, \alpha, \epsilon)$ will remain the same. In sharp contrast, learning an adversarially-robust classifier relies on the joint distribution of both the inputs and the labels.

Moreover, when the standard concentration function is translated into an upper bound on adversarial robustness, it is defined with respect to the set of imperfect classifiers $\mathcal{F}_\alpha$ (see Lemma 3.1). Note that the only restriction imposed by $\mathcal{F}_\alpha$ is that the risk of the classifier (or equivalently, the measure of the
corresponding error region) is at least $\alpha$. Note that, unlike adversarially robust learning, this does not consider whether the classifier is learnable. Thus, it is very likely that the optimal classifier implied by the standard concentration function cannot be produced by any supervised learning method. Suppose $\mathcal{F}_{\text{learn}}$ denotes the set of learnable classifiers. Then, $\text{AdvRob}_s(\mathcal{F}_{\alpha}, c)$ could be much higher than $\text{AdvRob}_s(\mathcal{F}_{\text{learn}}, c)$. In fact, it has been observed in [Mahlojifard et al. (2019b)] that the intrinsic robustness limit implied by concentration of measure is much higher than the adversarial robustness attained by state-of-the-art robust training methods on several image benchmarks.

**Gaussian Mixture Model.** We further illustrate the insufficiency of standard concentration under a simple Gaussian mixture model. Let $\mathcal{X} \subseteq \mathbb{R}^n$ be the input space and $\mathcal{Y} = \{-1, +1\}$ be the label space. Assume all the inputs are first generated according to a mixture of 2-Gaussian distribution: $x \sim \mu = \frac{1}{2}N(-\theta, \sigma^2I_n) + \frac{1}{2}N(\theta, \sigma^2I_n)$, then labeled by a concept function $c(x) = \text{sgn}(\theta^\top x)$, where $\theta \in \mathbb{R}^n$ and $\sigma \in \mathbb{R}$ are given parameters (this concept function is also the Bayes optimal classifier, which best separates the two Gaussian clusters). Theorem 3.2 proven in Appendix B.1 characterizes the optimal solution to the standard concentration problem under this assumed model.

**Theorem 3.2.** Consider the above Gaussian mixture model with $\ell_2$ perturbation metric. The optimal solution to the standard concentration problem 3.1) is a halfspace, either

$$
\mathcal{H}_- = \{x \in \mathcal{X} : \theta^\top x + b \cdot \|\theta\|_2 \leq 0\} \text{ or } \mathcal{H}_+ = \{x \in \mathcal{X} : \theta^\top x - b \cdot \|\theta\|_2 \geq 0\},
$$

where $b$ is a parameter depending on $\alpha$ and $\theta$ such that $\mu(\mathcal{H}_-) = \mu(\mathcal{H}_+) = \alpha$.

**Remark 3.3.** Theorem 3.2 suggests that for the Gaussian mixture model, the optimal subset achieving the smallest $\epsilon$-expansion under $\ell_2$-norm distance metric is a halfspace $\mathcal{H}$, which is far away from the decision boundary of the ground-truth labeling function $c(\cdot)$. Note that when translated into the intrinsic robustness problem, the corresponding optimal classifier $f$ has to be constructed by treating $\mathcal{H}$ as the only error region, or more precisely $f(x) = c(x)$ if $x \not\in \mathcal{H}$; otherwise, $f(x) \neq c(x)$.

This is counter-intuitive, however, if we consider the learnability of $f$. Since all the inputs in $\mathcal{H}$ and their neighbours share the same class label and are also far away from the decision boundary of $c(\cdot)$, examples that fall into $\mathcal{H}$ should be easily classified correctly using simple decision rules, such as k-nearest neighbour or maximum margin. This again confirms our claim that standard concentration is not sufficient for capturing a meaningful intrinsic robustness limit for a classification problem.

### 4 Incorporating Label Uncertainty in Intrinsic Robustness

In this section, we introduce our definition of label uncertainty and show how to include it in the intrinsic robustness measures. Let $(\mathcal{X}, \mu)$ be the input probability space and $\mathcal{Y} = \{1, 2, \ldots, k\}$ denote the complete set of labels. A function $\eta : \mathcal{X} \to [0, 1]^k$ is said to capture the full label distribution [Geng, 2016; Gao et al., 2017], if $[\eta(x)]_y$ corresponds to the description degree of $y$ to $x$ for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, and $\sum_{y \in [k]} [\eta(x)]_y = 1$ holds for any $x \in \mathcal{X}$. For classification tasks that rely on human labeling, one can approximate the label distribution with respect to any input by collecting human labels from multiple human annotators [Peterson et al., 2019]. When human uncertainty labels are not available, one can use methods, such as label distribution learning [Geng, 2016; Shen et al., 2017], to estimate the underlying label distribution $\eta(\cdot)$.

For any subset $E \in \text{pow}(\mathcal{X})$, we introduce the notion of label uncertainty to capture the average uncertainty level with respect to the label assignments of the inputs within $E$:

**Definition 4.1 (Label Uncertainty).** Let $(\mathcal{X}, \mu)$ be the input probability space and $\mathcal{Y} = \{1, 2, \ldots, k\}$ be the complete set of class labels. Suppose $c : \mathcal{X} \to \mathcal{Y}$ is a concept function that assigns each input $x$ a label $y \in \mathcal{Y}$. Assume $\eta : \mathcal{X} \to [0, 1]^k$ is the underlying label distribution function, where $[\eta(x)]_y$ represents the description degree of $y$ to $x$. For any subset $E \in \text{pow}(\mathcal{X})$ with measure $\mu(E) > 0$, the label uncertainty (LU) of $E$ with respect to $(\mathcal{X}, \mu)$, $c(\cdot)$ and $\eta(\cdot)$ is defined as:

$$
\text{LU}(E; \mu, c, \eta) = \frac{1}{\mu(E)} \int_E \left(1 - [\eta(x)]_{c(x)} + \max_{y \neq c(x)} [\eta(x)]_y\right) d\mu.
$$

We define $\text{LU}(E; \mu, c, \eta)$ as the average label uncertainty for all the examples that fall into $E$, where $1 - [\eta(x)]_{c(x)} + \max_{y \neq c(x)} [\eta(x)]_y$ represents the label uncertainty of a single example $\{x, c(x)\}$. The range of label uncertainty is $[0, 2]$. For a single input, label uncertainty of 0 suggests the assigned
label fully captures the underlying label distribution; label uncertainty of 1 means there are other classes as likely to be the ground-truth label as the assigned label; label uncertainty of 2 means the input is mislabeled and there is a different label that represents the ground-truth label.

State-of-the-art classification models are expected to more frequently misclassify inputs with large label uncertainty, as there is more discrepancy between their assigned labels and the underlying label distribution (see Section 6 for empirical evidence for this for CIFAR-10). Thus, to obtain a more realistic intrinsic robustness limit, we propose the following constrained concentration problem:

$$\min_{\mathcal{E} \in \text{pow}(\mathcal{X})} \mu(\mathcal{E}) \quad \text{subject to} \quad \mu(\mathcal{E}) \geq \alpha \quad \text{and} \quad \text{LU}(\mathcal{E}; \mu, c, \eta) \geq \gamma,$$

where $\gamma \in [0, 2]$ is a constant that will be determined based on the given classification problem. When $\gamma$ is set as zero, (4.1) degenerates to the standard concentration of measure problem.

Similar to the connection between the standard concentration function and $\text{AdvRob}_{\alpha}(\mathcal{F}_\alpha)$, the optimal value of (4.1) is equivalent to $1 - \text{AdvRob}_{\alpha}(\mathcal{F}_{\alpha, \gamma})$, where $\mathcal{F}_{\alpha, \gamma}$ denotes the set of classifiers with risk at least $\alpha$ and error region label uncertainty at least $\gamma$. As long as a classifier $f$ belongs to $\mathcal{F}_{\alpha, \gamma}$, it is guaranteed that $\text{AdvRob}_{\alpha}(f) \leq \text{AdvRob}_{\alpha}(\mathcal{F}_{\alpha, \gamma}) \leq \text{AdvRob}_{\alpha}(\mathcal{F}_\alpha)$. Although both $\text{AdvRob}_{\alpha}(\mathcal{F}_\alpha)$ and $\text{AdvRob}_{\alpha}(\mathcal{F}_{\alpha, \gamma})$ can serve as valid robustness upper bounds, the latter one would be able to capture a more meaningful intrinsic robustness limit, since it accounts for the fact that state-of-the-art classification models prone to misclassify inputs with higher label uncertainty.

5 Measuring Concentration with Label Uncertainty Constraints

This section introduces the proposed method for estimating the concentration of measure with label uncertainty constraints. Since directly solving (4.1) requires the knowledge of the underlying input distribution $\mu$ and the ground-truth label distribution function $\eta(\cdot)$, which are usually not available for classification problems, we consider the following empirical counterpart:

$$\min_{\mathcal{E} \in \mathcal{G}} \hat{\mu}_S(\mathcal{E}) \quad \text{subject to} \quad \hat{\mu}_S(\mathcal{E}) \geq \alpha \quad \text{and} \quad \text{LU}(\mathcal{E}; \hat{\mu}_S, c, \hat{\eta}) \geq \gamma,$$

where the search space is restricted to some specific collection of subsets $\mathcal{G} \subseteq \text{pow}(\mathcal{X})$, $\mu$ is replaced by the empirical distribution $\hat{\mu}_S$ with respect to a set of inputs sampled from $\mu$, and the empirical label distribution $\hat{\eta}(x)$ is considered as an empirical replacement of $\eta(x)$ for any given input $x \in \mathcal{S}$.

Next, we provide a theoretical analysis on the asymptotic behaviour of the proposed empirical estimator as in (5.1). In particular, we need to make use of the following definition of complexity penalty that is defined for some collection of subsets $\mathcal{G} \in \text{pow}(\mathcal{X})$. VC dimension and Rademacher complexity are commonly-used examples of such a complexity penalty.

**Definition 5.1** (Complexity Penalty). Let $\mathcal{G} \subseteq \text{pow}(\mathcal{X})$. We say $\phi : \mathbb{N} \times [0, 1] \rightarrow [0, 1]$ is a complexity penalty for $\mathcal{G}$, if for any $\delta \in (0, 1)$, it holds that

$$\Pr_{S \sim \mu^m} [\exists \mathcal{E} \in \mathcal{G} : |\hat{\mu}_S(\mathcal{E}) - \mu(\mathcal{E})| \geq \delta] \leq \phi(m, \delta).$$

Theorem 5.2 proved in Appendix [B.2] characterizes a generalization bound regarding the proposed label uncertainty estimate. More specifically, it shows that if $\mathcal{G}$ is not too complex and $\hat{\eta}$ is close to the ground-truth label distribution function $\eta$, the empirical estimate of label uncertainty $\text{LU}(\mathcal{E}; \hat{\mu}_S, c, \hat{\eta})$ is guaranteed to be close to the actual label uncertainty $\text{LU}(\mathcal{E}; \mu, c, \eta)$.

**Theorem 5.2** (Generalization of Label Uncertainty). Let $(\mathcal{X}, \mu)$ be a probability space and $\mathcal{G} \subseteq \text{pow}(\mathcal{X})$ be a collection of subsets of $\mathcal{X}$. Assume $\phi : \mathbb{N} \times [0, 1] \rightarrow [0, 1]$ is a complexity penalty for $\mathcal{G}$. If $\hat{\eta}(\cdot)$ is close to $\eta(\cdot)$ in $L^1$-norm with respect to $\mu$, i.e., $\int_{\mathcal{X}} |\eta(x) - \hat{\eta}(x)| d\mu \leq \delta_\eta$, where $\delta_\eta \in (0, 1)$ is a small constant, then for any $\alpha$, $\delta \in (0, 1)$ such that $\delta < \alpha$, we have

$$\Pr_{S \sim \mu^m} [\exists \mathcal{E} \in \mathcal{G} \quad \mu(\mathcal{E}) \geq \alpha : |\text{LU}(\mathcal{E}; \mu, c, \eta) - \text{LU}(\mathcal{E}; \hat{\mu}_S, c, \hat{\eta})| \leq \frac{4\delta + \delta_\eta}{\alpha - \delta}] \leq \phi(m, \delta).$$

Theorem 5.2 further implies the generalization of concentration under label uncertainty constraints. To be more specific, Theorem B.3 proved in Appendix [B.3] shows that the optimal value of the empirical label uncertainty constrained concentration problem (5.1) is close to the actual concentration, if both $\mathcal{G}$ and the collection of its $\epsilon$-expansions $\mathcal{G}_\epsilon = \{ \mathcal{E} : \mathcal{E} \in \mathcal{G} \}$ are not too complex.
When we conduct experiments on the CIFAR-10H dataset (Peterson et al., 2019), which contains soft labels for measuring human perceptual uncertainty for the 10,000 CIFAR-10 test images (Krizhevsky & Hinton, 2017), we increase both the complexity of the collection of subsets \( \mathcal{G} \) and the number of samples used for the empirical estimation, the optimal value of the empirical concentration problem (5.1) will converge to the actual concentration function with an error limit of \( \delta_t/\alpha \) on parameter \( \gamma \). That said, when the difference between the empirical label distribution \( \hat{\eta}(-) \) and the underlying label distribution \( \eta(-) \) is negligible, it is guaranteed that the optimal value of (5.1) converges to that of (4.1) asymptotically.

### 5.1 Concentration Estimation Algorithm

Although Theorem 5.3 and Remark 5.4 provide a general idea how to choose \( \mathcal{G} \) for measuring concentration, it still remains unclear how to solve the empirical concentration problem (5.1) for a specific perturbation metric. This section presents a heuristic algorithm for estimating the optimal value of (5.1) when the metric is \( \ell_2 \)-norm or \( \ell_\infty \)-norm. More specifically, we choose \( \mathcal{G} \) as the collection of union of balls for \( \ell_2 \)-norm distance metric (union of hypercubes for \( \ell_\infty \)-norm). It is worth noting that such choices of \( \mathcal{G} \) satisfy the condition required for the generalization of concentration theorem, since they are universal approximators for any set and the VC-dimensions of both \( \mathcal{G} \) and \( \mathcal{G}_r \) are both bounded (see Eisenstat & Angluin, 2007 and Devroye et al., 2013). The formal definitions of union of balls and union of hypercubes are given as follows:

**Definition 5.5 (Union of \( \ell_p \)-Balls).** Let \( p \geq 1 \). For any \( T \in \mathbb{Z}^+ \), define the union of \( T \) \( \ell_p \)-balls as

\[
\mathcal{B}(T; \ell_p) = \left\{ \bigcup_{t=1}^{T} \mathcal{B}_{\ell_p}(\mathbf{u}_t) : \forall t \in [T], (\mathbf{u}_t, r_t) \in \mathbb{R}^n \times \mathbb{R}_{\geq 0}^n \right\},
\]

When \( p = \infty \), \( \mathcal{B}(T; \ell_\infty) \) corresponds to the union of hypercubes.

Now the remaining task is how to solve (5.1) based on the selected collection of subsets \( \mathcal{G} \). Inspired by the algorithm for \( \ell_2 \) proposed in Mahloujarif et al. (2019b), we propose to place the balls (or the hypercubes) in a sequential manner, and searches for the best placement that satisfies the label uncertainty constraint using a greedy approach at each time. The pseudocode of the proposed searching algorithm is shown as Algorithm 1 in Appendix C. In particular, we initialize the feasible set of the hyperparameters \( \Omega \) as an empty set for each placement of balls (or hypercubes), then enumerate all the possible initial placements, \( S_{\text{init}}(\mathbf{u}, k) \), such that its empirical label uncertainty exceeds the given threshold \( \gamma \). Finally, among all the feasible ball (or hypercube) placements, we record the one that has the smallest \( \epsilon \)-expansion with respect to the empirical measure \( \hat{\mu} \). In this way, the input region produced by Algorithm 1 would serve as a good approximated solution to the empirical problem (5.1).

### 6 Experiments

We conduct experiments on the CIFAR-10H dataset (Peterson et al., 2019), which contains soft labels reflecting human perceptual uncertainty for the 10,000 CIFAR-10 test images (Krizhevsky & Hinton, 2017).
These soft labels can be regarded as an approximation of the label distribution function \( \eta(\cdot) \) at each given input, whereas the original CIFAR-10 test dataset provides the class labels given by the concept function \( c(\cdot) \). We report on experiments showing the connection between label uncertainty and classification error rates (Section 6.1) and that incorporating label uncertainty enables better intrinsic robustness estimates (Section 6.2). Section 6.3 demonstrates the possibility of improving model robustness by abstaining for inputs in high label uncertainty regions.

6.1 Error Regions have Larger Label Uncertainty

Figure 1(a) shows the label uncertainty scores for several images with both the soft labels from CIFAR-10H and the original class labels from CIFAR-10 (see Appendix D for more illustrations). Images with low uncertainty scores are typically easier for humans to recognize their class category (first row of Figure 1(a)), whereas images with high uncertainty scores look ambiguous or even misleading (second and third rows). Figure 1(b) shows the histogram of the label uncertainty distribution for all the 10,000 CIFAR-10 test examples. In particular, more than 80\% of the examples have label uncertainty scores below 0.1, suggesting the original class labels mostly capture the underlying label distribution well. However, around 2\% of the examples have label uncertainty scores exceeding 0.7, and some 400 images appear to be mislabeled with uncertainty scores above 1.2.

We hypothesize that ambiguous or misleading images should also be more likely to be misclassified as errors by state-of-the-art machine learning classifiers. That is, their induced error regions should have larger that typical label uncertainty. To test this hypothesis, we conduct experiments on CIFAR-10 and CIFAR-10H datasets. More specifically, we train different classification models, including intermediate models extracted at different epochs, using the CIFAR-10 training dataset, then empirically compute the standard risk, adversarial risk, and label uncertainty of the corresponding error region. The results are shown in Figure 2 (see Appendix E for experimental details).

Figures 2(a) and 2(b) demonstrate the relationship between label uncertainty and standard risk for various classifiers produced by standard training and adversarial training methods under \( \ell_\infty \) perturbations with \( \epsilon = 8/255 \). In addition, we plot the label uncertainty with error bars of randomly-selected images from the CIFAR-10 test dataset as a reference. As the model classification accuracy increases, the label uncertainty of its induced error region increases, suggesting the misclassified examples tend to have higher label uncertainty. This observation holds consistently for both standard and adversarially trained models with any tested network architecture. Figure 2(c) summarizes the error region label uncertainty with respect to the state-of-the-art adversarially robust models documented in RobustBench (Croce et al., 2020). Regardless of the perturbation type or the learning method, the average label uncertainty of their misclassified examples all falls into a range of \((0.17, 0.23)\), whereas the mean label uncertainty of all the testing CIFAR-10 data is less than 0.1. This supports our hypothesis that error regions of state-of-the-art classifiers tend to have larger label uncertainty, and our claim that intrinsic robustness estimates should account for labels.
6.2 Empirical Estimation of Intrinsic Robustness

In this section, we apply Algorithm 1 to estimate the intrinsic robustness limit for the CIFAR-10 dataset under $\ell_\infty$ perturbations with $\epsilon = 8/255$ and $\ell_2$ perturbations with $\epsilon = 0.5$. We set the label uncertainty threshold $\gamma = 0.17$ to roughly represent the error region label uncertainty of state-of-the-art classification models (see Figure 2). We adopt a 50/50 train-test split over the original 10,000 CIFAR-10 test images, and tune the parameter $T$ for each setting to obtain the best result (see Appendix E for experimental details).

Figure 3 demonstrates our intrinsic robustness estimates when choosing different values of $\alpha$. Note that we include the baseline estimates implied by standard concentration by setting $\gamma = 0$ in Algorithm 1 as opposed to our intrinsic robustness estimates with $\gamma = 0.17$. For a better illustration, we also plot the standard error and the robust accuracy of the state-of-the-art adversarially robust models in RobustBench (Croce et al., 2020). The $x$-axis stands for the empirical measure of the input region returned by Algorithm 1 whereas it represents the standard error for RobustBench models.

Compared with the baseline estimates, our label-uncertainty constrained intrinsic robustness estimates are uniformly lower across all the considered settings (similar results are obtained under other experimental settings, see Table 1 in Appendix D). Although both of these estimates can serve as legitimate upper bounds on the maximum achievable adversarial robustness for the given task, our estimate, which takes data labels into account, being closer to the robust accuracy achieved by state-of-the-art classifiers indicates it is a more accurate characterization of intrinsic robustness limit. For instance, under $\ell_2$ perturbation with $\epsilon = 0.5$, the best adversarially-trained classification model achieves approximately 73% robust accuracy with 10% clean error, whereas our estimate indicates that the maximum robustness one can hope for is about 83% as long as the classification model has at least 10% clean error. In contrast, the intrinsic robustness limit implied by standard concentration is as high as 88% for the same setting, which again shows the insufficiency of standard concentration.
6.3 Abstaining based on Label Uncertainty

Following the definition of label uncertainty, and our experimental results in the previous subsections, we expect classification models to have higher accuracy on examples with low label uncertainty. Here, we report on experiments to study the effect of abstaining based on label uncertainty on both clean and robust accuracies.

We use Carmon et al. (2019)’s state-of-the-art adversarially-trained classification model, which achieves 89.7% clean accuracy and 59.5% robust accuracy against $\ell_\infty$ perturbations with $\epsilon = 8/255$ on CIFAR-10 (additional experiments using a different classification model are provided in Appendix D). By sorting all the test CIFAR-10 images based on label uncertainty, we evaluate the model performance with respect to different percentages of included examples. Figure 4 shows the clean and robust accuracy curves of the considered classification model on different subsets of examples. The model achieves approximately 65% robust accuracy on the 9,000 test CIFAR-10 images with label uncertainty below 0.22, but only achieves slightly above 20% robust accuracy on the 1,000 images with label uncertainty greater than 0.22.

The accuracy curves shown in Figure 4 suggest a potential way to improve the robustness of classification systems is to enable the classifier an option to abstain on examples with high uncertainty score. Since the originally-assigned class labels of these examples are already disputable, it would be very hard to defend against adversarial perturbations to these examples. As an illustration, if we allow the robust classifier of Carmon et al. (2019) to abstain on the 2% of the test examples whose label uncertainty exceeds 0.7, the model clean accuracy will be improved from 89.7% to 90.3%, while the robust accuracy will increase from 59.5% to 60.4%. This is close to the maximum robust accuracy that can be achieved with a 2% abstention rate ($0.595/(1 - 0.02) = 0.607$). This result points to abstaining on examples in high label uncertainty regions as a promising path towards achieving adversarial robustness.

7 Conclusion

We argue that standard concentration fails to sufficiently capture intrinsic robustness since it ignores data labels. Based on the definition of label uncertainty, we observe that the error regions induced by state-of-the-art classification models all tend to have high label uncertainty. This motivates us to propose an empirical method to study the concentration behavior regarding the input regions with high label uncertainty, which results in more accurate intrinsic robustness measures for benchmark image classification tasks. Our experiments show the importance of considering labels in understanding intrinsic robustness, and further suggest that abstaining based on label uncertainty could be a potential method to improve the classifier accuracy and robustness.
Availability

An implementation of our method, and code for reproducing our experiments, is available under an open source license from:

https://github.com/xiaozhanguva/Intrinsic_robustness_label_uncertainty

Acknowledgements

This work was partially funded by an award from the National Science Foundation (NSF) SaTC program (Center for Trustworthy Machine Learning, #1804603).

References

Jean-Baptiste Alayrac, Jonathan Uesato, Po-Sen Huang, Alhussein Fawzi, Robert Stanforth, and Pushmeet Kohli. Are labels required for improving adversarial robustness? In NeurIPS, 2019.

Anish Athalye, Nicholas Carlini, and David Wagner. Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. In International Conference on Machine Learning, 2018.

Arjun Nitin Bhalgoji, Daniel Cullina, and Prateek Mittal. Lower bounds on adversarial robustness from optimal transport. In NeurIPS, 2019.

Christer Borell. The Brunn-Minkowski inequality in Gauss space. Inventiones mathematicae, 30(2):207–216, 1975.

Sebastien Bubeck, Yin Tat Lee, Eric Price, and Ilya Razenshteyn. Adversarial examples from computational constraints. In International Conference on Machine Learning, 2019.

Yair Carmon, Aditi Raghunathan, Ludwig Schmidt, John C Duchi, and Percy S Liang. Unlabeled data improves adversarial robustness. In NeurIPS, 2019.

Jeremy Cohen, Elan Rosenfeld, and Zico Kolter. Certified adversarial robustness via randomized smoothing. In International Conference on Machine Learning, 2019.

Francesco Croce and Matthias Hein. Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks. In International Conference on Machine Learning, pp. 2206–2216. PMLR, 2020.

Francesco Croce, Maksym Andriushchenko, Vikash Sehwag, Nicolas Flammarion, Mung Chiang, Prateek Mittal, and Matthias Hein. RobustBench: a standardized adversarial robustness benchmark. arXiv preprint arXiv:2010.09670, 2020.

Luc Devroye, László Györfi, and Gábor Lugosi. A probabilistic theory of pattern recognition, volume 31. Springer Science & Business Media, 2013.

Elvis Dohmatob. Generalized no free lunch theorem for adversarial robustness. In International Conference on Machine Learning, 2019.

David Eisenstat and Dana Angluin. The VC dimension of k-fold union. Information Processing Letters, 101(5):181–184, 2007.

Alhussein Fawzi, Hamza Fawzi, and Omar Fawzi. Adversarial vulnerability for any classifier. In NeurIPS, 2018.

Bin-Bin Gao, Chao Xing, Chen-Wei Xie, Jianxin Wu, and Xin Geng. Deep label distribution learning with label ambiguity. IEEE Transactions on Image Processing, 26(6):2825–2838, 2017.

Xin Geng. Label distribution learning. IEEE Transactions on Knowledge and Data Engineering, 28(7):1734–1748, 2016.
Justin Gilmer, Luke Metz, Fartash Faghri, Samuel S Schoenholz, Maithra Raghu, Martin Wattenberg, and Ian Goodfellow. Adversarial spheres. arXiv:1801.02774, 2018.

Ian Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In International Conference on Learning Representations, 2015.

Sven Gowal, Krishnamurthy Dvijotham, Robert Stanforth, Rudy Bunel, Chongli Qin, Jonathan Usato, Relja Arandjelovic, Timothy Mann, and Pushmeet Kohli. Scalable verified training for provably robust image classification. In IEEE International Conference on Computer Vision, 2019.

Chuan Guo, Mayank Rana, Moustapha Cisse, and Laurens van der Maaten. Countering adversarial images using input transformations. In International Conference on Learning Representations, 2018.

Alex Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. Technical report, University of Toronto, 2009.

Ryen Krusinga, Sohil Shah, Matthias Zwicker, Tom Goldstein, and David Jacobs. Understanding the (un)interpretability of natural image distributions using generative models. arXiv:1901.01499, 2019.

Michel Ledoux. Isoperimetry and Gaussian analysis. In Lectures on Probability Theory and Statistics. Springer, 1996.

Bai Li, Changyou Chen, Wenlin Wang, and Lawrence Carin. Certified adversarial robustness with additive noise. In NeurIPS, 2019.

Saeed Mahloujifar, Dimitrios Diochnos, and Mohammad Mahmoody. The curse of concentration in robust learning: Evasion and poisoning attacks from concentration of measure. In AAAI Conference on Artificial Intelligence, 2019a.

Saeed Mahloujifar, Xiao Zhang, Mohammad Mahmoody, and David Evans. Empirically measuring concentration: Fundamental limits on intrinsic robustness. In NeurIPS, 2019b.

Aleksander Mądry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In International Conference on Learning Representations, 2018.

Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami. Distillation as a defense to adversarial perturbations against deep neural networks. In IEEE Symposium on Security and Privacy, 2016.

Joshua C Peterson, Ruairidh M Battleday, Thomas L Griffiths, and Olga Russakovsky. Human uncertainty makes classification more robust. In IEEE International Conference on Computer Vision, 2019.

Jack Prescott, Xiao Zhang, and David Evans. Improved estimation of concentration under $\ell_p$-norm distance metrics using half spaces. In International Conference on Learning Representations, 2021.

Aditi Raghunathan, Jacob Steinhardt, and Percy Liang. Certified defenses against adversarial examples. In International Conference on Learning Representations, 2018.

Ali Shafahi, W. Ronny Huang, Christoph Studer, Soheil Feizi, and Tom Goldstein. Are adversarial examples inevitable? In International Conference on Learning Representations, 2019.

Wei Shen, Kai Zhao, Yilu Guo, and Alan Yuille. Label distribution learning forests. In NeurIPS, 2017.

Vladimir N Sudakov and Boris S Tsirelson. Extremal properties of half-spaces for spherically invariant measures. Zapiski Nauchnykh Seminarov Leningrad Otdel Mathematical Institute Steklov (LOMI), 41:14–24, 1974.
Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. In *International Conference on Learning Representations*, 2014.

Michel Talagrand. Concentration of measure and isoperimetric inequalities in product spaces. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 81(1):73–205, 1995.

Florian Tramer, Nicholas Carlini, Wieland Brendel, and Aleksander Madry. On adaptive attacks to adversarial example defenses. *arXiv:2002.08347*, 2020.

Eric Wong and Zico Kolter. Provable defenses against adversarial examples via the convex outer adversarial polytope. In *International Conference on Machine Learning*, 2018.

Eric Wong, Frank R Schmidt, Jan Hendrik Metzen, and Zico Kolter. Scaling provable adversarial defenses. In *NeurIPS*, 2018.

Dongxian Wu, Shu-Tao Xia, and Yisen Wang. Adversarial weight perturbation helps robust generalization. In *NeurIPS*, 2020.

Cihang Xie, Jianyu Wang, Zhishuai Zhang, Zhou Ren, and Alan Yuille. Mitigating adversarial effects through randomization. In *International Conference on Learning Representations*, 2018.

Hongyang Zhang, Yaodong Yu, Jiantao Jiao, Eric Xing, Laurent El Ghaoui, and Michael Jordan. Theoretically principled trade-off between robustness and accuracy. In *International Conference on Machine Learning*, 2019.

Huan Zhang, Hongge Chen, Chaowei Xiao, Sven Gowal, Robert Stanforth, Bo Li, Duane Boning, and Cho-Jui Hsieh. Towards stable and efficient training of verifiably robust neural networks. In *International Conference on Learning Representations*, 2020a.

Xiao Zhang, Jinghui Chen, Quanquan Gu, and David Evans. Understanding the intrinsic robustness of image distributions using conditional generative models. In *International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2020b.

### A Related Work

This section summarizes the work related to ours, beyond the brief background provided in the Introduction. First, we discuss the line of research aiming to develop robust classification models against adversarial examples. Then, we introduce the line of works which focus on understanding the intrinsic robustness limit.

#### A.1 Training Adversarially Robust Classifiers

Witnessing the vulnerability of modern machine learning models to adversarial examples, extensive studies have been carried out aiming to build classification models that can be robust against adversarial perturbations. Heuristic defense mechanisms (Goodfellow et al., 2015; Papernot et al., 2016; Guo et al., 2018; Xie et al., 2018; Madry et al., 2018) had been most popular until many of them were broken by stronger adaptive adversaries (Athalye et al., 2018; Tramer et al., 2020). The only scalable defense which seems to hold up well against adaptive adversaries is PGD-based adversarial training (Madry et al., 2018). Several variants of PGD-based adversarial training have been proposed, which either adopt different loss function (Zhang et al., 2019; Wu et al., 2020) or make use of additional training data (Carmon et al., 2019; Alayrac et al., 2019). Nevertheless, the best current adversarially-trained classifiers can only achieve around 60% robust accuracy on CIFAR-10 against $\ell_\infty$ perturbations with strength $\epsilon = 8/255$, even with additional training data (see the leaderboard in Croce et al., 2020).

To end the arms race between heuristic defenses and newly designed adaptive attacks that break them, certified defenses have been developed based on different approaches, including linear programming (Wong & Kolter, 2018; Wong et al., 2018), semidefinite programming (Raghunathan et al., 2018), interval bound propagation (Gowal et al., 2019; Zhang et al., 2020a), and randomized smoothing (Cohen et al., 2019; Li et al., 2019). Although certified defenses are able to train classifiers with robustness guarantees for input instances, most defenses can only scale to small networks and they usually come with sacrificed empirical robustness, especially for larger adversarial perturbations.
A.2 Theoretical Understanding on Intrinsic Robustness

Given the unsatisfactory status quo of building adversarially robust classification models, a line of research (Gilmer et al., 2018; Fawzi et al., 2018; Mahloujifar et al., 2019a; Shafahi et al., 2019; Dohmatob, 2019; Bhagoji et al., 2019) attempted to explain the adversarial vulnerability from a theoretical perspective. These works proved that as long as the input distribution is concentrated with respect to the perturbation metric, adversarially robust classifiers cannot exist. At the core of these results is the fundamental connection between the concentration of measure phenomenon and an intrinsic robustness limit that capture the maximum adversarial robustness with respect to some specific set of classifiers. For instance, (Gilmer et al., 2018) showed that for inputs sampled from uniform n-spheres, a model-independent robustness upper bound under the Euclidean distance metric can be derived using the Gaussian Isoperimetric Inequality (Sudakov & Tsirelson, 1974; Borell, 1975). Mahloujifar et al. (2019a) generalized their result to any concentrated metric probability space of inputs. Nevertheless, it is unclear how to apply these theoretical results to typical image classification tasks, since whether or not natural image distributions are concentrated is unknown.

To address this question, Mahloujifar et al. (2019b) proposed a general way to empirically measure the concentration for any input distribution using data samples, then employed it to estimate an intrinsic robustness limit for typical image benchmarks. By showing the existence of a large gap between the limit implied by concentration and the empirical robustness achieved by state-of-the-art adversarial training methods, Mahloujifar et al. (2019b) further concluded that concentration of measure can only explain a small portion of adversarial vulnerability of existing image classifiers. More recently, Prescott et al. (2021) further strengthened their conclusion by using the set of half-spaces to estimate the concentration function, which achieves enhanced estimation accuracy. Other related works (Fawzi et al., 2018; Krusinga et al., 2019; Zhang et al., 2020b) proposed estimating lower bounds on the concentration function, which achieves enhanced estimation accuracy. Other related works (Fawzi et al., 2018; Krusinga et al., 2019; Zhang et al., 2020b) proposed estimating lower bounds on the concentration of measure by approximating the underlying distribution using generative models. None of these works, however, consider data labels. Our main results show that data labels are essential for understanding intrinsic robustness limits.

B Proofs of Main Results

In this section, we provide detailed proofs of our main results, including Theorem 3.2, Theorem 5.2, Theorem 5.3 and Remark 5.4.

B.1 Proof of Theorem 3.2

In order to prove Theorem 3.2, we make use of the Gaussian Isoperimetric Inequality (Sudakov & Tsirelson, 1974; Borell, 1975). The proof of such inequality can be found in Ledoux (1996).

**Lemma B.1** (Gaussian Isoperimetric Inequality). Let \((\mathbb{R}^n, \mu)\) be the \(n\)-dimensional Gaussian space equipped with the \(\ell_2\)-norm distance metric. Consider an arbitrary subset \(\mathcal{E} \in \text{pow}(\mathbb{R}^n)\), suppose \(\mathcal{H}\) is a half space that satisfies \(\mu(\mathcal{H}) = \mu(\mathcal{E})\). Then for any \(\epsilon \geq 0\), we have

\[
\mu(\mathcal{E}_\epsilon) \geq \mu(\mathcal{H}_\epsilon) = \Phi(\Phi^{-1}(\mu(\mathcal{E})) + \epsilon),
\]

where \(\Phi(\cdot)\) is the cumulative distribution function of \(\mathcal{N}(0, 1)\) and \(\Phi^{-1}(\cdot)\) is its inverse function.

Now we are ready to prove Theorem 3.2.

**Proof of Theorem 3.2.** To begin with, we introduce the following notations. Let \(\mu_-\) be the probability measure for \(\mathcal{N}(-\Theta, \sigma^{-2}\mathbf{I}_n)\) and \(\mu_+\) be the probability measure for \(\mathcal{N}(\Theta, \sigma^2\mathbf{I}_n)\), then by definition, we have \(\mu = \mu_-/2 + \mu_+/2\). Consider the optimal subset \(\mathcal{E}^* = \text{argmin}_{\mathcal{E} \in \text{pow}(\mathbb{R}^n)} \{\mu_+(\mathcal{E}) : \mu(\mathcal{E}) \geq \alpha\}\).

Note that the standard concentration function \(h(\mu, \alpha, \epsilon)\) is monotonically increasing with respect to \(\alpha\), thus \(\mu(\mathcal{E}^*) = \alpha\) holds for any continuous \(\mu\). Let \(\alpha_- = \mu_-(\mathcal{E}^*)\) and \(\alpha_+ = \mu_+(\mathcal{E}^*)\). According to the Gaussian Isoperimetric Inequality Lemma B.1, it holds for any \(\epsilon \geq 0\) that

\[
\mu(\mathcal{E}_\epsilon^*) = \frac{1}{2}\mu_-(\mathcal{E}_\epsilon^*) + \frac{1}{2}\mu_+(\mathcal{E}_\epsilon^*) \geq \frac{1}{2}\Phi(\Phi^{-1}(\alpha_-) + \epsilon) + \frac{1}{2}\Phi(\Phi^{-1}(\alpha_+) + \epsilon).
\]

(B.1)

Note that the equality of (B.1) can be achieved if and only if \(\mathcal{E}^*\) is a half space.
Next, we show that there always exists a half space $\mathcal{H} \in \text{pow}(\mathcal{X})$ such that $\mu_-(\mathcal{H}) = \alpha_-$ and $\mu_+(\mathcal{H}) = \alpha_+$. Let $f_-(\cdot)$, $f_+(\cdot)$ be the PDFs of $\mu_-$ and $\mu_+$ respectively. For any $x \in \mathcal{X}$, $f_-(x)$ and $f_+(x)$ are always positive, thus we have

$$
\frac{f_+(x)}{f_-(x)} = \exp\left\{ -\frac{1}{2\sigma^2}(x - \theta)^\top (x - \theta) \right\} = \exp\left( \frac{2\theta^\top x}{\sigma^2} \right).
$$

This implies that the ratio of $f_+(x)/f_-(x)$ is monotonically increasing with respect to $\theta^\top x$.

Consider the following extreme half space $\mathcal{H}_- = \{x \in \mathcal{X} : \theta^\top x + b \cdot \|\theta\|_2 \leq 0\}$ such that $\mu(\mathcal{H}_-) = \alpha$. We are going to prove $\mu_-(\mathcal{H}_-) \geq \mu_-(\mathcal{E}^*) = \alpha_-$ and $\mu_+(\mathcal{H}_-) \leq \mu_+(\mathcal{E}^*) = \alpha_+$.

Consider the sets $\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C}$ and $(\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-$, we have

$$
\frac{\mu_+(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C})}{\mu_-((\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-)} \geq \inf_{x \in \mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C}} \exp\left( \frac{2\theta^\top x}{\sigma^2} \right) \geq \sup_{x \in (\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-} \left( \frac{2\theta^\top x}{\sigma^2} \right) \geq \mu_+((\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-).
$$

(B.2)

Note that we also have

$$
\mu_+(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C}) + \mu_-((\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-) = \mu_+((\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-) + \mu_-(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C})
$$

(B.3)

Thus, combining (B.2) and (B.3), we have

$$
\mu_+(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C}) \geq \mu_+((\mathcal{E}^*)\mathcal{C} \cap \mathcal{H}_-) \quad \text{and} \quad \mu_-(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C}) \leq \mu_-(\mathcal{E}^* \cap (\mathcal{H}_-)\mathcal{C})
$$

On the other hand, consider the half space $\mathcal{H}_+ = \{x \in \mathcal{X} : \theta^\top x - b \cdot \|\theta\|_2 \geq 0\}$ such that $\mu(\mathcal{H}_+) = \alpha$. Based on a similar technique, we can prove

$$
\mu_-(\mathcal{H}_+) \geq \mu_+(\mathcal{E}^*) = \alpha_+ \quad \text{and} \quad \mu_-(\mathcal{H}_+) \leq \mu_-(\mathcal{E}^*) = \alpha_-
$$

In addition, let $\mathcal{H} = \{x \in \mathcal{X} : w^\top x + b \leq 0\}$ be any half space such that $\mu(\mathcal{H}) = \alpha$. Since both $\mu_+$ and $\mu_-$ are continuous, as we rotate the half space (i.e., gradually increase the value of $w^\top \theta$), $\mu_-(\mathcal{H})$ and $\mu_+(\mathcal{H})$ will also change continuously. Therefore, it is guaranteed that there exists a half space $\mathcal{H} \in \text{pow}(\mathcal{X})$ such that $\mu_-(\mathcal{H}) = \alpha_-$ and $\mu_+(\mathcal{H}) = \alpha_+$. This further implies that the lower bound of (B.1) can be always be achieved.

Finally, since we have proved the optimal subset has to be a half space, the remaining task is to solve the following optimization problem:

$$
\min_{\mathcal{H} \in \text{pow}(\mathcal{X})} \frac{1}{2} \Phi^{-1}(\mu_-(\mathcal{H})) + \frac{1}{2} \Phi^{-1}(\mu_+(\mathcal{H})) + \epsilon
$$

s.t. $\mathcal{H} = \{x \in \mathcal{X} : w^\top x + b \leq 0\}$ and $\mu(\mathcal{H}) = \alpha$.

Construct function $g(u) = \Phi(\Phi^{-1}(u) + \epsilon) + \Phi(\Phi^{-1}(2\alpha - u) + \epsilon), \text{ where } u \in [0, 2\alpha]$. Based on the derivative of inverse function formula, we compute the derivative of $g$ with respect to $u$ as follows

$$
\frac{dg(u)}{du} = \frac{1}{\sqrt{2\pi}} \exp\left\{ -\frac{(\Phi^{-1}(u) + \epsilon)^2}{2} \right\} \cdot \frac{d\Phi^{-1}(u)}{du}
$$

$$
+ \frac{1}{\sqrt{2\pi}} \exp\left\{ -\frac{(\Phi^{-1}(2\alpha - u) + \epsilon)^2}{2} \right\} \cdot \frac{d\Phi^{-1}(2\alpha - u)}{du}
$$

$$
= \exp\left\{ -\frac{(\Phi^{-1}(u) + \epsilon)^2}{2} \right\} \cdot \exp\left\{ \frac{(\Phi^{-1}(u))^2}{2} \right\}
$$

$$
- \exp\left\{ -\frac{(\Phi^{-1}(2\alpha - u) + \epsilon)^2}{2} \right\} \cdot \exp\left\{ \frac{(\Phi^{-1}(2\alpha - u))^2}{2} \right\}
$$

$$
= \exp(-\epsilon^2/2) \cdot \exp\left( -\epsilon\Phi^{-1}(u) \right) - \exp\left( -\epsilon\Phi^{-1}(2\alpha - u) \right).
$$

Noticing the term $\exp(-\epsilon\Phi^{-1}(u))$ is monotonically decreasing with respect to $u$, we then know that $g(u)$ is monotonically increasing in $[0, \alpha]$ and monotonically decreasing in $[\alpha, 2\alpha]$. Therefore, this suggests that the optimal solution to (B.4) is achieved when $\mu_-(\mathcal{H})$ reaches its maximum or its minimum. According to the previous argument regarding the range of $\alpha_-$ and $\alpha_+$, we can immediately prove the optimality results of Theorem 3.2.

\[\square\]
B.2 Proof of Theorem 5.2

Proof of Theorem 5.2. For simplicity, denote by $lu(x; c, \eta) = 1 - [\eta(x)]_{c(x)} + \max_{y' \neq c(x)} [\eta(x)]_{y'}$ the label uncertainty of a given input $x$ with respect to $c(\cdot)$ and $\eta(\cdot)$. Let $\mathcal{E}$ be a subset in $\mathcal{G}$ such that $\mu(\mathcal{E}) \geq \alpha$ and $|\mu(\mathcal{E}) - \hat{\mu}(\mathcal{E})| \leq \delta$, where $\delta$ is a constant much smaller than $\alpha$. Then according to Definition 4.1, we can decompose the estimation error of label uncertainty as:

$$LU(\mathcal{E}; \mu, c, \eta) - LU(\mathcal{E}; \hat{\mu}_S, c, \hat{\eta}) = \frac{1}{\mu(\mathcal{E})} \int_\mathcal{E} lu(x; c, \eta) \, d\mu - \frac{1}{\hat{\mu}_S(\mathcal{E})} \int_\mathcal{E} lu(x; c, \hat{\eta}) \, d\hat{\mu}_S$$

$$= \left( \frac{1}{\mu(\mathcal{E})} - \frac{1}{\hat{\mu}_S(\mathcal{E})} \right) \cdot \int_\mathcal{E} lu(x; c, \eta) \, d\mu + \frac{1}{\hat{\mu}_S(\mathcal{E})} \int_\mathcal{E} [lu(x; c, \eta) - lu(x; c, \hat{\eta})] \, d\mu + \frac{1}{\hat{\mu}_S(\mathcal{E})} \left( \int_\mathcal{E} lu(x; c, \hat{\eta}) \, d\mu - \int_\mathcal{E} lu(x; c, \hat{\eta}) \, d\hat{\mu}_S \right).$$

Next, we upper bound the absolute value of the three components, respectively.

Consider the first term $I_1$. Note that $0 \leq lu(x; c, \eta) \leq 2$ for any $x \in \mathcal{X}$, thus we have $|\int_\mathcal{E} lu(x; c, \eta) \, d\mu| \leq 2\mu(\mathcal{E})$. Therefore, we have

$$|I_1| \leq \left| \frac{1}{\mu(\mathcal{E})} - \frac{1}{\hat{\mu}_S(\mathcal{E})} \right| \cdot 2\mu(\mathcal{E}) \leq \frac{2}{\mu(\mathcal{E})} \cdot |\mu(\mathcal{E}) - \hat{\mu}_S(\mathcal{E})|.$$

As for the second term $I_2$, the following inequality holds for any $x \in \mathcal{X}$

$$|\int_\mathcal{E} [lu(x; c, \eta) - lu(x; c, \hat{\eta})] \, d\mu| \leq \left| [\eta(x) - \tilde{\eta}(x)]_{c(x)} \right| + \max_{y' \neq c(x)} \left| [\eta(x)]_{y'} - \max_{y' \neq c(x)} [\tilde{\eta}(x)]_{y'} \right| \leq ||\eta(x) - \tilde{\eta}(x)||_1,$$

where the second inequality holds because $\max_{a_i} a_i - \max_{b_i} b_i \leq \max_{a_i} |a_i - b_i|$ for any $a, b \in \mathbb{R}^n$. Therefore, we can upper bound $|I_2|$ by

$$|I_2| \leq \frac{1}{\hat{\mu}_S(\mathcal{E})} \int_\mathcal{E} ||\eta(x) - \tilde{\eta}(x)||_1 \, d\mu \leq \frac{1}{\hat{\mu}_S(\mathcal{E})} \int_\mathcal{X} ||\eta(x) - \tilde{\eta}(x)||_1 \, d\mu \leq \frac{\delta}{\hat{\mu}_S(\mathcal{E})}.$$

For the last term $I_3$, since $0 \leq lu(x; c, \eta) \leq 2$ holds for any $x \in \mathcal{X}$, we have

$$|I_3| \leq 2 \cdot |\mu(\mathcal{E}) - \hat{\mu}_S(\mathcal{E})|.$$

Finally, putting pieces together, we have

$$|LU(\mathcal{E}; \mu, c, \eta) - LU(\mathcal{E}; \hat{\mu}_S, c, \hat{\eta})| \leq \frac{4}{\mu(\mathcal{E})} \cdot |\mu(\mathcal{E}) - \hat{\mu}_S(\mathcal{E})| + \frac{\delta}{\hat{\mu}_S(\mathcal{E})} \leq \frac{4\delta + \delta}{\alpha - \delta},$$

provided $\mu(\mathcal{E}) \geq \alpha$ and $|\mu(\mathcal{E}) - \hat{\mu}_S(\mathcal{E})| \leq \delta$. Making use of the definition of complexity penalty for $\mathcal{G}$ completes the proof of Theorem 5.2.

B.3 Proof of Theorem 5.3

Proof of Theorem 5.3. To begin with, we introduce the following notations. Let $h(\mu, c, \eta, \alpha, \gamma, \epsilon, \mathcal{G})$ be the optimal value and $g(\mu, c, \eta, \alpha, \gamma, \epsilon, \mathcal{G})$ be the optimal solution with respect to the following generalized concentration of measure problem with label uncertainty constraint:

$$\minimize_{\mathcal{E} \in \mathcal{G}} \mu(\mathcal{E}) \quad \text{subject to} \quad \mu(\mathcal{E}) \geq \alpha \quad \text{and} \quad LU(\mathcal{E}; \mu, c, \eta) \geq \gamma. \quad (B.5)$$
Note that the difference between (B.5) and (4.1) is that the feasible set of $\mathcal{E}$ is restricted to some collection of subsets $\mathcal{G} \subseteq \text{pow}(\mathcal{X})$. Correspondingly, we let $h(\tilde{\mu}_S, c, \tilde{\eta}, \alpha, \gamma, \epsilon, \mathcal{G})$ and $g(\tilde{\mu}_S, c, \tilde{\eta}, \alpha, \gamma, \epsilon, \mathcal{G})$ be the optimal value and optimal solution with respect to the empirical optimization problem (5.1).

Let $\mathcal{E} = g(\mu, c, \eta, \alpha + \delta, \gamma + \delta', \epsilon, \mathcal{G})$ and $\hat{\mathcal{E}} = g(\tilde{\mu}_S, c, \tilde{\eta}, \alpha, \gamma, \epsilon, \mathcal{G})$, where $\delta'$ will be specified later. Note that when these optimal sets do not exist, we can select a set for which the expansion is arbitrarily close to the optimum, then every step of the proof will apply to this variant. According to the definition of complexity penalty, we have

$$\Pr_{S \sim \mu_m}[|\tilde{\mu}_S(\hat{\mathcal{E}}) - \mu(\hat{\mathcal{E}})| \geq \delta] \leq \phi(m, \delta). \quad (B.6)$$

Since $\tilde{\mu}_S(\hat{\mathcal{E}}) \geq \alpha$ by definition, (B.6) implies that

$$\Pr_{S \sim \mu_m}[\mu(\hat{\mathcal{E}}) \leq \alpha - \delta] \leq \phi(m, \delta). \quad (B.7)$$

In addition, according to Theorem 5.2 for any $\delta \in (0, \alpha/2)$, we have

$$\Pr_{S \sim \mu_m}\left[\left|\text{LU}(\hat{\mathcal{E}}; \mu, c, \eta) - \text{LU}(\mathcal{E}; \tilde{\mu}_S, c, \tilde{\eta})\right| \leq \frac{4\delta + \delta_\eta}{\alpha - 2\delta}\right] \leq 2\phi(m, \delta), \quad (B.8)$$

where the inequality holds because of (B.7) and the union bound. Since $\text{LU}(\hat{\mathcal{E}}; \tilde{\mu}_S, c, \tilde{\eta}) \geq \gamma$ by definition, (B.8) implies that

$$\Pr_{S \sim \mu_m}\left[\text{LU}(\mathcal{E}; \mu, c, \eta) \leq \gamma - \frac{4\delta + \delta_\eta}{\alpha - 2\delta}\right] \leq 2\phi(m, \delta). \quad (B.9)$$

Based on the definition of the concentration function $h$, combining (B.7) and (B.9) and making use of the union bound, we have

$$\Pr_{S \sim \mu_m}[\mu(\hat{\mathcal{E}}) \leq h(\mu, c, \eta, \alpha - \delta, \gamma - \delta', \epsilon, \mathcal{G})] \leq 3\phi(m, \delta), \quad (B.10)$$

where we set $\delta' = \frac{4\delta + \delta_\eta}{\alpha - 2\delta}$. Note that according to the definition of $\phi_\epsilon$, we have

$$\Pr_{S \sim \mu_m}[|\mu(\hat{\mathcal{E}}) - \mu_S(\hat{\mathcal{E}})| \leq \delta] \leq \phi_\epsilon(m, \delta), \quad (B.11)$$

thus combining (B.10) and (B.11) by union bound, we have

$$\Pr_{S \sim \mu_m}[\tilde{\mu}_S(\hat{\mathcal{E}}) \leq h(\mu, c, \eta, \alpha, \gamma - \delta', \epsilon, \mathcal{G}) - \delta] \leq 3\phi(m, \delta) + \phi_\epsilon(m, \delta). \quad (B.12)$$

This completes the proof of one-sided inequality of Theorem 5.3. The other side of Theorem 5.3 can be proved using the same technique. In particular, we have

$$\Pr_{S \sim \mu_m}[\tilde{\mu}_S(\hat{\mathcal{E}}) \geq h(\mu, c, \eta, \alpha + \delta, \gamma + \delta', \epsilon, \mathcal{G}) + \delta] \leq 3\phi(m, \delta) + \phi_\epsilon(m, \delta). \quad (B.13)$$

Combining (B.12) and (B.13) by union bound completes the proof.$\Box$

### B.4 Proof of Remark 5.4

Before presenting the proofs, we first lay out the formal statement of Remark 5.4 in Theorem B.2. The proof technique of Theorem B.2 is inspired by Theorem 5.5 in Mahloujifar et al. (2019b).

**Theorem B.2** (Formal Statement of Remark 5.4). Consider the input metric probability space $(\mathcal{X}, \mu, \Delta)$, the concept function $c$ and the label distribution function $\eta$. Let $\{\mathcal{G}(T)\}_{T \in \mathbb{N}}$ be a series of collection of subsets over $\mathcal{X}$. For any $T \in \mathbb{N}$, assume $\phi^T$ and $\phi^T_\mathcal{G}$ are complexity penalties for $\mathcal{G}(T)$ and $\mathcal{G}_\mathcal{G}(T)$ respectively, and $\tilde{\eta}$ is a function such that $\int_X \|	ilde{\eta}(x) - \eta(x)\|_1 dx \leq \delta_\eta$.

Define $h(\mu, c, \eta, \alpha, \gamma, \epsilon, \mathcal{G}) = \inf_{\mathcal{E} \subseteq \mathcal{P}(\mathcal{X})} \{\mu(\mathcal{E}) \geq \alpha, \text{LU}(\mathcal{E}; \mu, c, \eta) \geq \gamma\}$ to be the constrained concentration function. We simply write $h(\mu, c, \eta, \alpha, \gamma, \epsilon)$ when $\mathcal{G} = \text{pow}(\mathcal{X})$. Given a sequence of datasets $\{S_T\}_{T \in \mathbb{N}}$, where $S_T$ consists of $(m(T))$ i.i.d. samples from $\mu$ and a sequence of real numbers $\{\delta(T)\}_{T \in \mathbb{N}}$ with $\delta(T) \in (0, \alpha/2)$, if the following assumptions holds:

1. $\sum_{T=1}^{\infty} \phi^T(m(T), \delta(T)) < \infty$
2. $\sum_{T=1}^{\infty} \phi_T^T(m(T), \delta(T)) < \infty$

3. $\lim_{T \to \infty} \delta(T) = 0$

4. $\lim_{T \to \infty} h(\mu, c, \eta, \alpha, \gamma, \epsilon, G(T)) = h(\mu, c, \eta, \alpha, \gamma, \epsilon)$

5. $h$ is locally continuous w.r.t. $\alpha$ and $\gamma$ at $(\mu, c, \eta, \alpha, \gamma \pm \delta_\gamma/\alpha, \epsilon, \text{pow}(X))$.

Then with probability 1, we have

$$h(\mu, c, \eta, \alpha, \gamma - \delta_\gamma/\alpha, \epsilon) \leq \lim_{T \to \infty} h(\mu_{S_T}, c, \eta, \alpha, \gamma, \epsilon, G(T)) \leq h(\mu, c, \eta, \alpha, \gamma + \delta_\gamma/\alpha, \epsilon).$$

To prove Theorem B.2, we need to make use of the following Borel-Cantelli Lemma.

**Lemma B.3** (Borel-Cantelli Lemma). Let $\{E_T\}_{T \in \mathbb{N}}$ be a series of events such that $\sum_{T=1}^{\infty} \Pr[E_T] < \infty$. Then with probability 1, only finite number of events will occur.

Now we are ready to prove Theorem B.2.

**Proof of Theorem B.2.** Let $E_T$ be the event such that

$$h(\mu, c, \eta, \alpha - \delta(T), \gamma - \delta'(T), \epsilon, G(T)) - \delta(T) > h(\tilde{\mu}_{S_T}, c, \tilde{\eta}, \alpha, \gamma, \epsilon, G(T))$$

and

$$h(\mu, c, \eta, \alpha + \delta(T), \gamma + \delta'(T), \epsilon, G(T)) + \delta(T) < h(\tilde{\mu}_{S_T}, c, \tilde{\eta}, \alpha, \gamma, \epsilon, G(T)).$$

Let $\delta'(T) = (4\delta(T) + \delta_\gamma)/(\alpha - 2\delta(T))$ for any $T \in \mathbb{N}$. Since $\delta(T) < \alpha/2$, thus according to Theorem 3.3 for any $T \in \mathbb{N}$, we have

$$\Pr[E_T] \leq 6\phi_T^T(m(T), \delta(T)) + 2\phi_T^T(m(T), \delta(T))) > 0.$$

By Assumptions 1 and 2, this further implies

$$\sum_{T=1}^{\infty} \Pr[E_T] \leq 6 \sum_{T=1}^{\infty} \phi_T^T(m(T), \delta(T)) + 2 \sum_{T=1}^{\infty} \phi_T^T(m(T), \delta(T))) < \infty.$$

Thus according to Lemma B.3, we know that there exists some $j \in \mathbb{N}$ such that for all $T \geq j$,

$$h(\mu, c, \eta, \alpha - \delta(T), \gamma - \delta'(T), \epsilon, G(T)) - \delta(T) \leq h(\tilde{\mu}_{S_T}, c, \tilde{\eta}, \alpha, \gamma, \epsilon, G(T)) + \delta(T),$$

(B.14)

holds with probability 1. In addition, by Assumptions 3, 4 and 5, we have

$$\lim_{T \to \infty} h(\mu, c, \eta, \alpha - \delta(T), \gamma - \delta'(T), \epsilon, G(T))$$

$$= \lim_{T_1 \to \infty} \lim_{T_2 \to \infty} h(\mu, c, \eta, \alpha - \delta(T_1), \gamma - \delta'(T_1), \epsilon, G(T_2))$$

$$= \lim_{T_1 \to \infty} h(\mu, c, \eta, \alpha - \delta(T_1), \gamma - \delta'(T_1), \epsilon)$$

$$= h(\mu, c, \eta, \alpha, \gamma - \delta_\gamma/\alpha, \epsilon),$$

where the second equality is due to Assumption 4 and the last equality is due to Assumptions 3 and 5. Similarly, we have

$$\lim_{T \to \infty} h(\mu, c, \eta, \alpha + \delta(T), \gamma + \delta'(T), \epsilon, G(T)) = h(\mu, c, \eta, \alpha, \gamma + \delta_\gamma/\alpha, \epsilon).$$

Therefore, let $T$ goes to $\infty$ in (B.14), we have

$$h(\mu, c, \eta, \alpha, \gamma - \delta_\gamma/\alpha, \epsilon) \leq \lim_{T \to \infty} h(\tilde{\mu}_{S_T}, c, \tilde{\eta}, \alpha, \gamma, \epsilon, G(T)) \leq h(\mu, c, \eta, \alpha, \gamma + \delta_\gamma/\alpha, \epsilon).$$

**C Pseudocode of the Proposed Algorithm**

The pseudocode of the proposed searching algorithm for the empirical label uncertainty constrained concentration problem (5.1) is shown in Algorithm 1.

---

1 It is worth noting that this assumption is satisfied for any family of collections of subsets that is a universal approximator, such as kernel SVMs and decision trees.
Algorithm 1: Heuristic Search for Robust Error Region under $\ell_p (p \in \{2, \infty\})$

| Input | a set of labeled inputs $\{x, c(x), \overline{y}(x)\}_{x \in \mathcal{S}}$, parameters $\alpha, \gamma, \epsilon, T$ |
|-------|--------------------------------------------------------------------------------------------------|
| $\tilde{E}$ | $\{\}$, $\tilde{S}_{\text{init}}$ | $\{\}$, $\tilde{S}_{\text{exp}}$ | $\{\}$ |
| for $t = 1, 2, \ldots, T$ do | $k_{\text{lower}} \leftarrow \lceil (\alpha|\mathcal{S}| - |\tilde{S}_{\text{init}}|)/(T - t + 1) \rceil$, $k_{\text{upper}} \leftarrow (\alpha|\mathcal{S}| - |\tilde{S}_{\text{init}}|)$; |
| for $u \in \mathcal{S}$ do | $\Omega \leftarrow \{\}$; |
| for $k \in [k_{\text{lower}}, k_{\text{upper}}]$ do | $r_k (u) \leftarrow$ compute the $\ell_p$ distance from $u$ to the $k$-th nearest neighbour in $\mathcal{S} \setminus \tilde{S}_{\text{init}}$; |
| $\tilde{S}_{\text{init}} (u, k) \leftarrow \{x \in \mathcal{S} \setminus \tilde{S}_{\text{init}} : \|x - u\|_2 \leq r_k (u)\}$; |
| $\tilde{S}_{\text{exp}} (u, k) \leftarrow \{x \in \mathcal{S} \setminus \tilde{S}_{\text{exp}} : \|x - u\|_2 \leq r_k (u) + \epsilon\}$; |
| if $\text{LU}(\tilde{S}_{\text{init}} (u, k), \tilde{S}_{\text{exp}}, \alpha, \epsilon) \geq \gamma$ then | insert $(u, k)$ into $\Omega$; |
| $(\hat{u}, \hat{k}) \leftarrow \text{argmin}_{(u, k) \in \Omega} \{|\tilde{S}_{\text{exp}} (u, k)| - |\tilde{S}_{\text{init}} (u, k)|\}$; |
| $\tilde{E} \leftarrow \tilde{E} \cup \text{Ball}(\hat{u}, r_{\hat{k}} (\hat{u}))$; |
| $\tilde{S}_{\text{init}} \leftarrow \tilde{S}_{\text{init}} \cup \tilde{S}_{\text{init}} (\hat{u}, \hat{k})$, $\tilde{S}_{\text{exp}} \leftarrow \tilde{S}_{\text{exp}} \cup \tilde{S}_{\text{exp}} (\hat{u}, \hat{k})$; |

Output: $\tilde{E}$

**D Other Experiments**

This appendix provides additional experimental results, supporting our arguments in Section 6.

Visualization of label uncertainty. Figure 5 shows some CIFAR-10 images with the original CIFAR-10 labels and the CIFAR-10H human uncertainty labels. The label uncertainty score is computed based on Definition 4.1 and provided under each image.

There are a few examples with high label uncertainty, whose CIFAR-10 label contradicts with the CIFAR-10H soft label (see the first two images in Figure 5(a)), indicating they are actually mislabeled. The images with uncertainty scores around 1.0 do appear to be images that are difficult for human to recognize, whereas images with lowest uncertainty scores look clearly representative of the labeled class. These observations show the usefulness of the proposed label uncertainty definition.

Estimation of Intrinsic Robustness. Table 1 summarizes our estimated intrinsic robustness limits produced by Algorithm 1 for different hyperparameter settings. In particular, we set $\alpha = 0.05$ and $\gamma = 0.17$ to roughly reflect the standard error and the label uncertainty of the error regions with respect to the state-of-the-art classification models (see Figure 2), use $\epsilon \in \{10^{-3} \times 255, 10^{-2} \times 255, 10^{-1} \times 255\}$ for $\ell_\infty$ and $\epsilon \in \{0.5, 1.0, 1.5\}$ for $\ell_2$. Note that we also compare our estimate with the intrinsic robustness limit implied by the standard concentration by setting $\gamma = 0$ for each setting.

We perform a 50/50 train-test split on the CIFAR-10 test images: we obtain the optimal subset with the smallest $\epsilon$-expansion on the training dataset based on Algorithm 1, and evaluate it on the testing dataset. We report both the empirical measure of the optimally-found subset (Empirical Risk in Table 1), and the translated intrinsic robustness estimate. These results show that our estimation of intrinsic robustness generalizes from the training data to the testing data, and support the argument that our estimate is a more accurate characterization of intrinsic robustness compared with standard one.

Abstaining based on label uncertainty. Figure 6 shows the effect of abstaining based on label uncertainty using Wu et al. (2020)’s state-of-the-art adversarially-trained classification model under $\ell_2$ perturbation with $\epsilon = 0.5$. The accuracy curves show a similar trend to those presented in Section 6.3, which again suggests that abstaining on examples with high label uncertainty is a promising way to improve model robustness.
Figure 5: Illustration of human uncertainty labels and label uncertainty of CIFAR-10 test images. Each subfigure shows a group of images with a certain level of uncertainty score.

Figure 6: Test accuracy curves for the adversarially-trained classification model (Wu et al., 2020) under $\ell_2$ perturbations with $\epsilon = 0.5$ on CIFAR-10 with respect to varying percentage of included examples based on label uncertainty: (a) include the set of examples with lowest label uncertainty; (b) include the set of examples with highest label uncertainty. Label uncertainty thresholds are indicated corresponding to the percentage value of {0.8, 0.9, 0.98} for (a) and {0.02, 0.1, 0.2} for (b).
Table 1: Summary of the main results using our method for different settings on CIFAR-10 dataset. We conduct 5 repeated trials for each setting to record the mean statistics and its standard deviation.

| Metric | $\alpha$ | $\epsilon$ | $\gamma$ | $T$ | Empirical Risk (%) | Intrinsic Robustness (%) |
|--------|---------|------------|----------|-----|-------------------|------------------------|
|        |         |            |          |     | training | testing | training | testing |
| $\ell_\infty$ | 0.05 | 4/255 | 0.0 | 5 | 5.80 ± 0.04 | 4.50 ± 0.21 | 93.48 ± 0.10 | 93.86 ± 0.26 |
|         |       |           | 0.17 | 5 | 5.84 ± 0.10 | 5.06 ± 0.82 | 92.03 ± 0.45 | 92.61 ± 1.12 |
| $\ell_2$  | 0.05 | 8/255 | 0.0 | 10 | 5.77 ± 0.01 | 4.76 ± 0.27 | 92.89 ± 0.11 | 92.36 ± 0.33 |
|         |       |           | 0.17 | 10 | 5.77 ± 0.02 | 4.85 ± 0.58 | 90.91 ± 0.53 | 90.98 ± 1.03 |
|         |       | 16/255 | 0.0 | 5 | 5.68 ± 0.04 | 5.30 ± 0.33 | 88.44 ± 0.47 | 87.89 ± 1.24 |
|         |       |           | 0.17 | 5 | 5.67 ± 0.25 | 4.79 ± 0.75 | 81.96 ± 1.69 | 83.83 ± 2.37 |
|         | 0.5    |           |       |     |           |          |         |          |
|         | 1.0    |           |       |     |           |          |         |          |
|         | 1.5    |           |       |     |           |          |         |          |

E Detailed Experimental Settings

In this section, we specify the details of the experiments presented in Section 6. The robustness results of all the adversarially-trained models from RobustBench (Croce et al., 2020) are evaluated using the auto attack (Croce & Hein, 2020). All of our experiments are conducted using a GPU server with a NVIDIA GeForce RTX 2080 Ti Graphics card.

Error Region Label Uncertainty. We explain the experimental details of Figure 2. For standard trained classifiers, we implemented five neural network architecture, including a 4-layer neural net with two convolutional layers and two fully-connected layers (small), a 7-layer neural net with four convolutional layers and three fully-connected layers (large), a ResNet-18 architecture (resnet18), ResNet-50 architecture (resnet50) and a WideResNet-34-10 architecture (wideresnet). We trained the small and large model using an Adam optimizer with initial learning rate 0.005, whereas we trained the resnet18, resnet50 and wideresnet model using a SGD optimizer with initial learning rate 0.01. All models are trained using a piece-wise learning rate schedule with a decaying factor of 10 at epoch 50 and epoch 75, respectively. For Figure 2(a), we plotted the label uncertainty and standard risk for the intermediate models obtained at epochs 5, 10, ..., 100 for each architecture. In addition, we also randomly selected different subsets of inputs with empirical measure of 0.05, 0.10, ..., 0.95 and plotted their corresponding label uncertainty with error bars.

For adversarially trained classifiers, we implemented the vanilla adversarial training method (Madry et al., 2018) and the adversarial training method with adversarial weight perturbation (Wu et al., 2020), which are denoted as AT and AT-AWP in Figure 2(b), respectively. Both ResNet-18 (resnet18) and WideResNet-34-10 (wideresnet) architecture are implemented for each training method. A 10-step PGD attack (PGD-10) with step size 2/255 and maximum perturbation size 8/255 is used for each model during training. In addition, each model is trained for 200 epochs using a SGD optimizer with initial learning rate 0.1 and piece-wise learning rate schedule with a decaying factor of 10 at epoch 100 and epoch 150. We record the intermediate models at epoch 10, 20, ..., 200 respectively.

Estimation of Intrinsic Robustness. For Figure 3, we first conduct a 50/50 train-test split over the 10,000 CIFAR-10 test images, then run Algorithm 1 for each setting on the training dataset to obtain the optimal subset. Here, we choose the value of $\alpha \in \{0.01, 0.02, \ldots, 0.15\}$ and tune the parameter $T$ for each $\alpha$ parameter. Next, we evaluate the empirical measure of the optimally-searched subset (denoted by empirical risk in Figure 3) and the empirical measure of its $\epsilon$-expansion using the testing dataset, and translate it into an intrinsic robustness estimate. Finally, we plot the empirical risk and the estimated intrinsic robustness for each parameter setting in Figure 3.