RATT: LEVERAGING UNLABELED DATA TO GUARANTEE GENERALIZATION

Saurabh Garg, Sivaraman Balakrishnan, J. Zico Kolter, Zachary C. Lipton
Carnegie Mellon University
{sgarg2,sbalakri,zkolter,zlipton}@andrew.cmu.edu

ABSTRACT

To assess generalization, machine learning scientists typically either (i) bound the generalization gap and, after training, use the empirical risk to obtain a bound on the true risk; or (ii) validate empirically on holdout data. However, (i) typically yields vacuous guarantees for overparameterized models. Furthermore, (ii) shrinks the training set and its guarantee erodes with each re-use of the holdout set. In this paper, we introduce a method that leverages unlabeled data to produce non-vacuous bounds. After augmenting our (labeled) training set with randomly labeled fresh examples, we train in the standard fashion. Because models tend to fit true labels before noisy labels, we reach a point where the error on the clean training data is low but the error on the noisy training data is high. Our bound translates the (high) error on the noisy data to a (tight) post-hoc upper bound on the true risk. Theoretically, we prove that our bound holds with 0-1 loss minimization and with gradient-descent-trained linear classifiers. Empirically, for deep networks applied to canonical computer vision and NLP tasks, our bound provides non-vacuous generalization guarantees that track actual performance closely. This work provides practitioners with an option for certifying the generalization of deep nets even when unseen labeled data is unavailable and provides theoretical insights into the relationship between random label noise and generalization.

1 INTRODUCTION

Typically, machine learning scientists establish generalization in one of two ways. One approach, favored by learning theorists, places an *a priori* bound on the gap between the empirical and true risks, usually in terms of the complexity of the hypothesis class. After fitting the model on the available data, one can plug in the empirical risk to obtain a guarantee on the true risk. The second approach, favored by practitioners, involves splitting the available data into training and holdout partitions, fitting the models on the former and estimating the population risk with the latter.

Surely, both approaches are useful, with the former providing theoretical insights and the latter guiding the development of a vast array of practical technology. Nevertheless, both methods have drawbacks. Most *a priori* generalization bounds rely on uniform convergence and thus fail to explain the ability of deep neural networks to generalize (Zhang et al., 2016; Nagarajan & Kolter, 2019b). On the other hand, risk estimates based on holdout sets lose their validity with successive re-use of the holdout data due to adaptive overfitting (Murphy, 2012; Dwork et al., 2015), although recent empirical studies suggest that on large benchmark datasets, adaptive overfitting is surprisingly absent (Recht et al., 2019). Moreover, provisioning a holdout dataset restricts the amount of labeled data available for training.

In this paper, we propose Randomly Assign, Train and Track (RATT), a new method that leverages unlabeled data to provide a *post-training* bound on the true risk (i.e., the population error). Here, we assign random labels to a fresh batch of unlabeled data, augmenting the clean training dataset with these randomly labeled points. Next, we train on this data, following standard risk minimization practices. Finally, we track the error on the randomly labeled portion of training data, estimating the error on the mislabeled portion and using this quantity to upper bound the population error. Because, in practice, overparameterized deep networks tend to fit clean data before fitting mislabeled data, our procedure yields tight bounds in the early phases of learning.

Our work derives inspiration from recent observations on deep learning with noisy data (Rolnick et al., 2017; Arpit et al., 2017). Specifically, even when training data is contaminated by a small amount of mislabeled data, overparameterized networks nevertheless generalize well when trained with early stopping and weight decay (Hu et al., 2019; Li et al., 2019). Also, when training with noisy labels, overparameterized models tend to fit the clean training data first before eventually fitting the mislabeled data (Liu et al., 2020; Arora et al., 2019). Due to these phenomena, we can provide non-vacuous bounds.

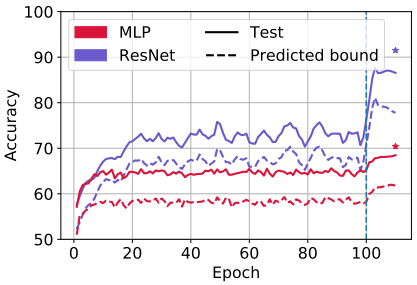


Figure 1: **Predicted lower bound on the clean population error** with ResNet and MLP on binary CIFAR. Results aggregated over 5 seeds. '*' denotes the best test performance achieved when training with only clean data and the same hyperparameters (except for the stopping point). The bound predicted by RATT (in Theorem 1) closely tracks the population accuracy on clean data.

Counterintuitively, we guarantee generalization by guaranteeing overfitting. Specifically, we prove that Empirical Risk Minimization (ERM) with 0-1 loss leads to lower error on the mislabeled training data than on unseen mislabeled data. Thus, if despite minimizing the loss on the combined training data, we nevertheless have high error on the mislabeled portion, then the (mislabeled) population error will be even higher. Then, by complementarity, the (clean) population error must be low. Finally, we show how to obtain this guarantee using randomly labeled (vs mislabeled data), thus enabling us to incorporate unlabeled data. To expand the applicability of our idea beyond ERM on 0-1 error, we prove corresponding results for a linear classifier trained by gradient descent to minimize squared loss. Because we make no assumptions on the data distribution, our results on linear models hold for more complex models such as kernel regression and neural networks in the NTK regime (Jacot et al., 2018; Du et al., 2018; Chizat et al., 2019).

Addressing practical deep learning models, while our guarantee requires a (reasonable) assumption, our experiments verify that the bound yields non-vacuous guarantees that track test error across several major architectures on a range of benchmark datasets for computer vision and Natural Language Processing (NLP). Moreover, we confirm the *early learning* phenomenon in standard SGD training and illustrate the effectiveness of early stopping in avoiding interpolation to mislabeled data while maintaining fit on the training data, strengthening the guarantee provided by our method.

To be clear, we do not advocate RATT as a blanket replacement for the holdout approach. Our main contribution is to introduce a new theoretical perspective on generalization and to provide a method that may be applicable even when the holdout approach is unavailable. Of interest, unlike generalization bounds based on uniform-convergence that restrict the complexity of the hypothesis class (Neyshabur et al., 2018; 2015; 2017b; Bartlett et al., 2017; Nagarajan & Kolter, 2019a), our *post hoc* bounds depend only on the fit to mislabeled data.

Preliminaries Suppose we have a multiclass classification problem with the input domain $\mathcal{X} \subseteq \mathbb{R}^d$ and label space $\mathcal{Y} = \{1, 2, \ldots, k\}$. For binary classification, we will use $\mathcal{Y} = \{-1, 1\}$. By $\mathcal{D}$ and $p_{\mathcal{D}}(\cdot)$, we denote the distribution over $\mathcal{X} \times \mathcal{Y}$ and the corresponding probability density function (pdf), respectively. A dataset $S := \{(x_i, y_i)\}_{i=1}^n \sim \mathcal{D}^n$ contains n points sampled i.i.d. from $\mathcal{D}$. By $\mathcal{S}$, we denote the (uniform) empirical distribution over points in S, and more generally, we use caligraphic symbols to denote the empirical distributions corresponding to a given dataset. Let $\mathcal{F}$ be a class of hypotheses mapping $\mathcal{X}$ to $\mathbb{R}^k$. A *training algorithm* $\mathcal{A}$: takes a dataset S, and returns a classifier $f(\mathcal{A}, S) \in \mathcal{F}$. When the context is clear, we drop the parenthesis for convenience. Given a classifier f and datum (x, y), we denote the 0-1 error (i.e., classification error) on that point by $\mathcal{E}(f(x), y) := \mathbb{I}\left[y \notin \arg\max_{j \in \mathcal{Y}} f_j(x)\right]$, We express the *population error* on $\mathcal{D}$ as $\mathcal{E}_{\mathcal{D}}(f) := \mathbb{E}_{(x,y)\sim\mathcal{D}}\left[\mathcal{E}(f(x), y)\right]$ and the *empricial error* on S as $\mathcal{E}_{\mathcal{S}}(f) := \mathbb{E}_{(x,y)\sim\mathcal{S}}\left[\mathcal{E}(f(x), y)\right] = \frac{1}{n}\sum_{i=1}^n \mathcal{E}(f(x_i), y_i)$.

Throughout the paper, we consider a *random label assignment* procedure: draw $x \sim \mathcal{D}_{\mathcal{X}}$ (the underlying distribution over $\mathcal{X}$), and then assign a label randomly sampled from the underlying marginal over $\mathcal{Y}$, i.e., $y \sim \mathcal{D}_{\mathcal{Y}}$ (the underlying distribution over $\mathcal{Y}$). For a distribution with uniform label marginal, this procedure assigns labels uniformly at random. We denote a randomly labeled dataset by $\widetilde{S} := \{(x_i, y_i)\}_{i=1}^m \sim \widetilde{\mathcal{D}}^m$, where $\widetilde{\mathcal{D}} := \mathcal{D}_{\mathcal{X}} \times \mathcal{D}_{\mathcal{Y}}$ is the distribution of randomly labeled data. By $\mathcal{D}'$, we denote the mislabeled distribution that corresponds to selecting examples (x, y) according to $\mathcal{D}$ and then re-assigning the label by sampling among the incorrect labels $y' \neq y$.

2 GENERALIZATION BOUND FOR RATT

We now present our generalization bound for ERM on the 0-1 loss (full proofs in App. C). Consider any function $R : \mathcal{F} \to \mathbb{R}$, e.g., a regularizer that penalizes some measure of complexity for functions in class $\mathcal{F}$. For any dataset T, ERM returns the classifier $\widehat{f}$ that minimizes the empirical error:

$$\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{T}}(f) + \lambda R(f)\,, \tag{1}$$

where λ is a regularization constant. To begin, we focus on binary classification with balanced classes. Assume we have a clean dataset $S \sim \mathcal{D}^n$ of n points and a randomly labeled dataset $\widetilde{S} \sim \widetilde{D}^m$ of $m(< n)$ points. Because the classes are balanced, labels in $\widetilde{S}$ are assigned uniformly at random. We show that with 0-1 loss minimization on the union of S and $\widetilde{S}$, we obtain a classifier whose population error (on $\mathcal{D}$) on the original data distribution is upper bounded by a function of the empirical errors on clean data $\mathcal{E}_{\mathcal{S}}$ (lower is better) and on randomly labeled data $\mathcal{E}_{\widetilde{\mathcal{S}}}$ (higher is better):

Theorem 1. *Assume we perform ERM as in* (1) *on $S \cup \widetilde{S}$ and obtain a classifier $\widehat{f}$. Then for any $\delta > 0$, with probability at least $1 - \delta$ we have $\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + 1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + \left(\sqrt{2}\mathcal{E}_{\widetilde{S}}(\widehat{f}) + 2 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}}$.*

Because the labels in $\widetilde{S}$ are assigned randomly, the error $\mathcal{E}_{\widetilde{\mathcal{S}}}(f)$ for any fixed predictor f (not dependent on $\widetilde{S}$) will be approximately 1/2. Note that if ERM produces a classifier that has not fit to the randomly labeled data, then $(1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}))$ will be approximately 0, and our error will be determined by the fit to clean data. In short, this theorem tells us that if after training on both clean and randomly labeled data, we achieve low error on the clean data but high error (close to $1/2$) on the randomly labeled data, then low population error is guaranteed. Our proof strategy unfolds in two steps. First, we bound $\mathcal{E}_{\mathcal{D}}(\widehat{f})$ in terms of the error on the mislabeled subset of $\widetilde{S}$. Next, we show that this quantity can be accurately estimated using only clean and randomly labeled data. Refer to App. B for a short proof.

Comparison with Rademacher bound Our bound in Theorem 4 shows that we can upper bound the clean population error of a classifier by estimating the its accuracy on the clean and randomly labeled portions of the training data. Next, we show that our bound's dominating term is upper bounded by the *Rademacher complexity* (Shalev-Shwartz & Ben-David, 2014), a standard distribution dependent complexity measure.

Proposition 1. *Fix a randomly labeled dataset $\widetilde{S} \sim \widetilde{\mathcal{D}}^m$. Then for any classifier $f \in \mathcal{F}$ (possibly dependent on $\widetilde{S}$) and for any $\delta > 0$, with probability at least $1 - \delta$ over random draws of $\widetilde{S}$, we have $1 - 2\mathcal{E}_{\widetilde{S}}(f) \leqslant \mathbb{E}_{\epsilon,x}\left[\sup_{f \in \mathcal{F}}\left(\frac{\sum_i \epsilon_i f(x_i)}{m}\right)\right] + \sqrt{\frac{2\log(\frac{2}{\delta})}{m}}$, where ϵ is drawn from a uniform distribution over $\{-1, 1\}^m$ and x is drawn from $\mathcal{D}_{\mathcal{X}}^m$.*

In other words, the proposition above highlights that the accuracy on the randomly labeled data is never larger than the Rademacher complexity of $\mathcal{F}$ w.r.t. the underlying distribution over $\mathcal{X}$, implying that our bound is never looser than a Rademacher complexity based bound.

Extension to multiclass classification Thus far, we have addressed binary classification. We now extend these results to the multiclass setting with balanced classes. As before, we obtain datasets S and $\widetilde{S}$. Here, random labels are assigned uniformly among all classes.

Theorem 2. *For any regularization function R, assume we perform regularized ERM as in* (1) *on $S \cup \widetilde{S}$ and obtain a classifier $\widehat{f}$. For a multiclass classification problem with k classes and uniform label marginal, for any $\delta > 0$, with probability at least $1 - \delta$, we have $\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + (k-1)\left(1 - \frac{k}{k-1}\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f})\right) + c\sqrt{\frac{\log(\frac{4}{\delta})}{2m}}$, for some constant $c \leqslant (2k + \sqrt{k} + \frac{m}{n\sqrt{k}})$.*

We first discuss the implications of Theorem 2. Besides empirical error on clean data, the dominating term in the above expression is given by $(k-1)\left(1 - \frac{k}{k-1}\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f})\right)$. For any predictor f (not dependent on $\widetilde{S}$), the term $\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f})$ would be approximately $(k-1)/k$ and for $\widehat{f}$, the difference now evaluates to the accuracy of the randomly labeled data.

Generalization Bound for RATT with Gradient Descent For simplicity, we consider binary classification with $\mathcal{X} = \mathbb{R}^d$. Define a linear function $f(x; w) := w^T x$ for some $w \in \mathbb{R}^d$ and $x \in \mathcal{X}$. Given training set S, we suppose that the parameters of the linear function are obtained via gradient descent on the following problem:

$$\mathcal{L}_S(w; \lambda) := \sum_{i=1}^{n} (w^T x_i - y_i)^2 + \lambda \|w\|_2^2 \,, \tag{2}$$

where $\lambda \geqslant 0$ is a regularization parameter. For a given training set S, we use $S_{(i)}$ to denote the training set S with the i^{th} point removed. We now introduce one stability condition:

Condition 1 (Hypothesis Stability)**.** *We have β hypothesis stability if our training algorithm $\mathcal{A}$ satisfies the following:* $\forall i \in \{1, 2, \ldots, n\}, \quad \mathbb{E}_{\mathcal{S},(x,y)\in\mathcal{D}} \left[\left| \mathcal{E}\left(f(x), y\right) - \mathcal{E}\left(f_{(i)}(x), y\right) \right| \right] \leqslant \frac{\beta}{n}$, *where $f_{(i)} := f(\mathcal{A}, S_{(i)})$ and $f := f(\mathcal{A}, S)$.*

This condition is similar to a notion of stability called *hypothesis stability* (Bousquet & Elisseeff, 2002; Kearns & Ron, 1999; Elisseeff et al., 2003). This condition is mild and does not guarantee generalization. We discuss the implications in more detail in App. D.

Now we present the main result of this section. As before, we assume access to a clean dataset $S = \{(x_i, y_i)\}_{i=1}^{n} \sim \mathcal{D}^n$ and randomly labeled dataset $\widetilde{S} = \{(x_i, y_i)\}_{i=n+1}^{n+m} \sim \widetilde{\mathcal{D}}^m$. Let $\boldsymbol{X} = [x_1, x_2, \cdots, x_{m+n}]$ and $\boldsymbol{y} = [y_1, y_2, \cdots, y_{m+n}]$. Fix a positive learning rate η such that $\eta \leqslant 1/\left(\left\|\boldsymbol{X}^T\boldsymbol{X}\right\|_{\text{op}} + \lambda^2\right)$ and an initialization $w_0 = 0$. Consider the following gradient descent iterates to minimize objective (2) on $S \cup \widetilde{S}$: $w_t = w_{t-1} - \eta \nabla_w \mathcal{L}_{S\cup\widetilde{S}}(w_{t-1}; \lambda) \quad \forall t = 1, 2, \ldots$ Then we have $\{w_t\}$ converge to the limiting solution $\widehat{w} = \left(\boldsymbol{X}^T\boldsymbol{X} + \lambda \boldsymbol{I}\right)^{-1} \boldsymbol{X}^T \boldsymbol{y}$. Define $\widehat{f}(x) := f(x; \widehat{w})$.

Theorem 3. *Assume that this gradient descent algorithm satisfies Condition 1 with $\beta = \mathcal{O}(1)$. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of datasets $\widetilde{S}$ and S, we have:*

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + 1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + \left(\sqrt{2}\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + 1 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}} + \sqrt{\frac{4}{\delta}\left(\frac{1}{m} + \frac{3\beta}{m+n}\right)}\,.$$

With a mild regularity condition, we establish the same bound on GD training with squared loss, notably the same dominating term on the population error, as in Theorem 4.

Empirical Study and Implications Having established our framework theoretically, we now demonstrate its utility experimentally. Here, we include results for wide networks in the NTK regime where our guarantee holds. We confirm that our bound is not only valid, but closely tracks the generalization error. In App. E, we show that in practical deep learning, optimizing cross-entropy loss by SGD, the expression for our (0-1) ERM bound nevertheless tracks test performance closely and in numerous binary and multiclass classification tasks on diverse models and datasets is never violated empirically.

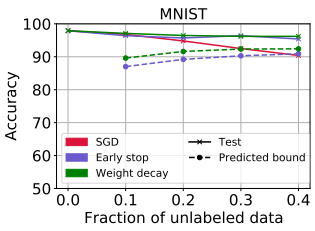


Figure 2: Accuracy and RATT bound (in Theorem 1) at $\delta = 0.1$ vs fraction of unlabeled data for a 2-layer wide network trained with SGD on binary MNIST.

We consider MNIST binary classification with a wide 2-layer fully-connected network. In experiments with SGD training on MSE loss without early stopping or weight decay regularization, we find that adding extra randomly label data hurts the unseen clean performance (Fig. 2(b)). Additionally, due to the perfect fit on the training data, our bound is rendered vacuous. However, with early stopping (or weight decay), we observe close to zero performance difference with additional randomly labeled data. Alongside, we obtain tight bounds on the accuracy on unseen clean data paying only a small price to negligible for incorporating randomly labeled data. Similar results hold for SGD and GD and when cross-entropy loss is substituted for MSE (ref. App. E).

Conclusion and Future Work Our work introduces a new approach for obtaining generalization bounds that do not directly depend on the underlying complexity of the model class. While our empirical findings and theoretical results with 0-1 loss (and squared loss GD training) hold absent further assumptions and shed light on why the bound may apply for more general models, we hope to extend our proof that overfitting (in terms classification error) to the finite sample of mislabeled data occurs with SGD training on broader classes of models and loss functions.

REFERENCES

Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. Tensorflow: A system for large-scale machine learning. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, pp. 265–283, 2016.

Karim Abou-Moustafa and Csaba Szepesvári. An exponential efron-stein inequality for lq stable learning rules. *arXiv preprint arXiv:1903.05457*, 2019.

Alnur Ali, J Zico Kolter, and Ryan J Tibshirani. A continuous-time view of early stopping for least squares. *arXiv preprint arXiv:1810.10082*, 2018.

Alnur Ali, Edgar Dobriban, and Ryan J Tibshirani. The implicit regularization of stochastic gradient flow for least squares. *arXiv preprint arXiv:2003.07802*, 2020.

Zeyuan Allen-Zhu, Yuanzhi Li, and Yingyu Liang. Learning and generalization in overparameterized neural networks, going beyond two layers. In *Advances in neural information processing systems*, pp. 6158–6169, 2019.

Sanjeev Arora, Rong Ge, Behnam Neyshabur, and Yi Zhang. Stronger generalization bounds for deep nets via a compression approach. *arXiv preprint arXiv:1802.05296*, 2018.

Sanjeev Arora, Simon S Du, Wei Hu, Zhiyuan Li, and Ruosong Wang. Fine-grained analysis of optimization and generalization for overparameterized two-layer neural networks. *arXiv preprint arXiv:1901.08584*, 2019.

Devansh Arpit, Stanislaw Jastrzebski, Nicolas Ballas, David Krueger, Emmanuel Bengio, Maxinder S Kanwal, Tegan Maharaj, Asja Fischer, Aaron Courville, Yoshua Bengio, et al. A closer look at memorization in deep networks. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 233–242. JMLR. org, 2017.

Yamini Bansal, Gal Kaplun, and Boaz Barak. For self-supervised learning, rationality implies generalization, provably. *arXiv preprint arXiv:2010.08508*, 2020.

Rémi Bardenet, Odalric-Ambrym Maillard, et al. Concentration inequalities for sampling without replacement. *Bernoulli*, 21(3):1361–1385, 2015.

Peter L Bartlett, Dylan J Foster, and Matus J Telgarsky. Spectrally-normalized margin bounds for neural networks. In *Advances in neural information processing systems*, pp. 6240–6249, 2017.

Olivier Bousquet and André Elisseeff. Stability and generalization. *Journal of machine learning research*, 2(Mar):499–526, 2002.

Lenaic Chizat and Francis Bach. Implicit bias of gradient descent for wide two-layer neural networks trained with the logistic loss. In *Conference on Learning Theory*, pp. 1305–1338. PMLR, 2020.

Lenaic Chizat, Edouard Oyallon, and Francis Bach. On lazy training in differentiable programming. In *Advances in Neural Information Processing Systems*, pp. 2937–2947, 2019.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*, 2018.

Simon Du, Jason Lee, Haochuan Li, Liwei Wang, and Xiyu Zhai. Gradient descent finds global minima of deep neural networks. In *International Conference on Machine Learning*, pp. 1675–1685. PMLR, 2019.

Simon S Du, Xiyu Zhai, Barnabas Poczos, and Aarti Singh. Gradient descent provably optimizes over-parameterized neural networks. *arXiv preprint arXiv:1810.02054*, 2018.

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 symposium on Theory of computing*, pp. 117–126, 2015.

Gintare Karolina Dziugaite and Daniel M Roy. Computing nonvacuous generalization bounds for deep (stochastic) neural networks with many more parameters than training data. *arXiv preprint arXiv:1703.11008*, 2017.

André Elisseeff, Massimiliano Pontil, et al. Leave-one-out error and stability of learning algorithms with applications. *NATO science series sub series iii computer and systems sciences*, 190:111–130, 2003.

Jerome Friedman and Bogdan E Popescu. Gradient directed regularization for linear regression and classification. Technical report, Technical Report, Statistics Department, Stanford University, 2003.

Suriya Gunasekar, Jason Lee, Daniel Soudry, and Nathan Srebro. Implicit bias of gradient descent on linear convolutional networks. *arXiv preprint arXiv:1806.00468*, 2018a.

Suriya Gunasekar, Blake Woodworth, Srinadh Bhojanapalli, Behnam Neyshabur, and Nathan Srebro. Implicit regularization in matrix factorization. In *2018 Information Theory and Applications Workshop (ITA)*, pp. 1–10. IEEE, 2018b.

Moritz Hardt, Ben Recht, and Yoram Singer. Train faster, generalize better: Stability of stochastic gradient descent. In *International Conference on Machine Learning*, pp. 1225–1234. PMLR, 2016.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep Residual Learning for Image Recognition. In *Computer Vision and Pattern Recognition (CVPR)*, 2016.

Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8): 1735–1780, 1997.

Wassily Hoeffding. Probability inequalities for sums of bounded random variables. In *The Collected Works of Wassily Hoeffding*, pp. 409–426. Springer, 1994.

Wei Hu, Zhiyuan Li, and Dingli Yu. Simple and effective regularization methods for training on noisily labeled data with generalization guarantee. *arXiv preprint arXiv:1905.11368*, 2019.

Wei Hu, Lechao Xiao, Ben Adlam, and Jeffrey Pennington. The surprising simplicity of the early-time learning dynamics of neural networks. *arXiv preprint arXiv:2006.14599*, 2020.

Arthur Jacot, Franck Gabriel, and Clément Hongler. Neural tangent kernel: Convergence and generalization in neural networks. In *Advances in neural information processing systems*, pp. 8571–8580, 2018.

Ziwei Ji and Matus Telgarsky. The implicit bias of gradient descent on nonseparable data. In *Conference on Learning Theory*, pp. 1772–1798. PMLR, 2019.

Michael Kearns and Dana Ron. Algorithmic stability and sanity-check bounds for leave-one-out cross-validation. *Neural computation*, 11(6):1427–1453, 1999.

Alex Krizhevsky and Geoffrey Hinton. Learning Multiple Layers of Features from Tiny Images. Technical report, Citeseer, 2009.

Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-Based Learning Applied to Document Recognition. *Proceedings of the IEEE*, 86, 1998.

Mingchen Li, Mahdi Soltanolkotabi, and Samet Oymak. Gradient descent with early stopping is provably robust to label noise for overparameterized neural networks. *arXiv preprint arXiv:1903.11680*, 2019.

Mingchen Li, Mahdi Soltanolkotabi, and Samet Oymak. Gradient descent with early stopping is provably robust to label noise for overparameterized neural networks. In *International Conference on Artificial Intelligence and Statistics*, pp. 4313–4324. PMLR, 2020.

Yuanzhi Li and Yingyu Liang. Learning overparameterized neural networks via stochastic gradient descent on structured data. In *Advances in Neural Information Processing Systems*, pp. 8157–8166, 2018.

Sheng Liu, Jonathan Niles-Weed, Narges Razavian, and Carlos Fernandez-Granda. Early-learning regularization prevents memorization of noisy labels. *arXiv preprint arXiv:2007.00151*, 2020.

Andrew Maas, Raymond E Daly, Peter T Pham, Dan Huang, Andrew Y Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In *Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies*, pp. 142–150, 2011.

Colin McDiarmid. *On the method of bounded differences*, pp. 148–188. London Mathematical Society Lecture Note Series. Cambridge University Press, 1989. doi: 10.1017/CBO9781107359949.008.

Sayan Mukherjee, Partha Niyogi, Tomaso Poggio, and Ryan Rifkin. Learning theory: stability is sufficient for generalization and necessary and sufficient for consistency of empirical risk minimization. *Advances in Computational Mathematics*, 25(1):161–193, 2006.

Kevin P Murphy. *Machine Learning: A Probabilistic Perspective*. MIT Press, 2012.

Vaishnavh Nagarajan and J Zico Kolter. Deterministic pac-bayesian generalization bounds for deep networks via generalizing noise-resilience. *arXiv preprint arXiv:1905.13344*, 2019a.

Vaishnavh Nagarajan and J Zico Kolter. Uniform convergence may be unable to explain generalization in deep learning. In *Advances in Neural Information Processing Systems*, pp. 11615–11626, 2019b.

Preetum Nakkiran, Gal Kaplun, Dimitris Kalimeris, Tristan Yang, Benjamin L Edelman, Fred Zhang, and Boaz Barak. Sgd on neural networks learns functions of increasing complexity. *arXiv preprint arXiv:1905.11604*, 2019.

Preetum Nakkiran, Behnam Neyshabur, and Hanie Sedghi. The deep bootstrap: Good online learners are good offline generalizers. *arXiv preprint arXiv:2010.08127*, 2020.

Gergely Neu and Lorenzo Rosasco. Iterate averaging as regularization for stochastic gradient descent. In *Conference On Learning Theory*, pp. 3222–3242. PMLR, 2018.

Behnam Neyshabur, Ryota Tomioka, and Nathan Srebro. Norm-based capacity control in neural networks. In *Conference on Learning Theory*, pp. 1376–1401, 2015.

Behnam Neyshabur, Srinadh Bhojanapalli, David McAllester, and Nathan Srebro. Exploring generalization in deep learning. *arXiv preprint arXiv:1706.08947*, 2017a.

Behnam Neyshabur, Srinadh Bhojanapalli, and Nathan Srebro. A pac-bayesian approach to spectrally-normalized margin bounds for neural networks. *arXiv preprint arXiv:1707.09564*, 2017b.

Behnam Neyshabur, Zhiyuan Li, Srinadh Bhojanapalli, Yann LeCun, and Nathan Srebro. The role of over-parametrization in generalization of neural networks. In *International Conference on Learning Representations*, 2018.

Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, Alban Desmaison, Andreas Kopf, Edward Yang, Zachary DeVito, Martin Raison, Alykhan Tejani, Sasank Chilamkurthy, Benoit Steiner, Lu Fang, Junjie Bai, and Soumith Chintala. Pytorch: An imperative style, high-performance deep learning library. In *Advances in Neural Information Processing Systems 32*, 2019.

Matthew E. Peters, Mark Neumann, Mohit Iyyer, Matt Gardner, Christopher Clark, Kenton Lee, and Luke Zettlemoyer. Deep contextualized word representations. In *Proc. of NAACL*, 2018.

Benjamin Recht, Rebecca Roelofs, Ludwig Schmidt, and Vaishaal Shankar. Do imagenet classifiers generalize to imagenet? In *International Conference on Machine Learning*, pp. 5389–5400. PMLR, 2019.

David Rolnick, Andreas Veit, Serge Belongie, and Nir Shavit. Deep learning is robust to massive label noise. *arXiv preprint arXiv:1705.10694*, 2017.

Shai Shalev-Shwartz and Shai Ben-David. *Understanding machine learning: From theory to algorithms*. Cambridge university press, 2014.

Shai Shalev-Shwartz, Ohad Shamir, Nathan Srebro, and Karthik Sridharan. Learnability, stability and uniform convergence. *The Journal of Machine Learning Research*, 11:2635–2670, 2010.

Jack Sherman and Winifred J Morrison. Adjustment of an inverse matrix corresponding to a change in one element of a given matrix. *The Annals of Mathematical Statistics*, 21(1):124–127, 1950.

Daniel Soudry, Elad Hoffer, Mor Shpigel Nacson, Suriya Gunasekar, and Nathan Srebro. The implicit bias of gradient descent on separable data. *The Journal of Machine Learning Research*, 19(1): 2822–2878, 2018.

Arun Suggala, Adarsh Prasad, and Pradeep K Ravikumar. Connecting optimization and regularization paths. In *Advances in Neural Information Processing Systems*, pp. 10608–10619, 2018.

Alexandre B Tsybakov et al. On nonparametric estimation of density level sets. *The Annals of Statistics*, 25(3):948–969, 1997.

Thomas Wolf, Lysandre Debut, Victor Sanh, Julien Chaumond, Clement Delangue, Anthony Moi, Pierric Cistac, Tim Rault, Rémi Louf, Morgan Funtowicz, Joe Davison, Sam Shleifer, Patrick von Platen, Clara Ma, Yacine Jernite, Julien Plu, Canwen Xu, Teven Le Scao, Sylvain Gugger, Mariama Drame, Quentin Lhoest, and Alexander M. Rush. Transformers: State-of-the-art natural language processing. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations*, pp. 38–45, Online, October 2020. Association for Computational Linguistics. URL https://www.aclweb.org/anthology/2020.emnlp-demos.6.

Yuan Yao, Lorenzo Rosasco, and Andrea Caponnetto. On early stopping in gradient descent learning. *Constructive Approximation*, 26(2):289–315, 2007.

Chiyuan Zhang, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals. Understanding deep learning requires rethinking generalization. *arXiv preprint arXiv:1611.03530*, 2016.

Wenda Zhou, Victor Veitch, Morgane Austern, Ryan P Adams, and Peter Orbanz. Non-vacuous generalization bounds at the imagenet scale: a pac-bayesian compression approach. *arXiv preprint arXiv:1804.05862*, 2018.

SUPPLEMENTARY MATERIAL

A DISCUSSION AND CONNECTIONS TO PRIOR WORK

Implicit bias in deep learning Several recent lines of research attempt to explain the generalization of neural networks despite massive overparameterization via the *implicit bias* of gradient descent (Soudry et al., 2018; Gunasekar et al., 2018a;b; Ji & Telgarsky, 2019; Chizat & Bach, 2020). Noting that even for overparameterized linear models, there exist multiple parameters capable of overfitting the training data (with arbitrarily low loss), of which some generalize well and others do not, they seek to characterize the favored solution. Notably, Soudry et al. (2018) finds that for linear networks, gradient descent converges (slowly) to the max margin solution. A complementary line of work focuses on the early phases of training, finding both empirically (Rolnick et al., 2017; Arpit et al., 2017) and theoretically (Arora et al., 2019; Li et al., 2020; Liu et al., 2020) that even in the presence of a small amount of mislabeled data, gradient descent is biased to fit the clean data first during initial phases of training. However, to best our knowledge, no prior work leverages this phenomenon to obtain generalization guarantees on the clean data, which is the primary focus of our work. Our method exploits this phenomenon to produce non-vacuous generalization bounds. Even when we cannot prove *a priori* that models will fit the clean data well while performing badly on the mislabeled data, we can observe that it indeed happens (often in practice), and thus, *a posteriori*, provide tight bounds on the population error. Moreover, by using regularizers like early stopping or weight decay, we can accentuate this phenomenon, enabling our framework to provide even tighter guarantees.

Non-vacuous generalization bounds In light of the inapplicability of traditional complexity-based bounds to deep neural networks (Zhang et al., 2016; Nagarajan & Kolter, 2019b), researchers have investigated alternative strategies to provide non-vacuous generalization bounds for deep nets (Neyshabur et al., 2015; 2017b;a; 2018; Dziugaite & Roy, 2017; Bartlett et al., 2017; Arora et al., 2018; Li & Liang, 2018; Allen-Zhu et al., 2019; Zhou et al., 2018; Nagarajan & Kolter, 2019a; Nakkiran et al., 2020). However, these bounds typically remain numerically loose relative to the true generalization error. However, (Dziugaite & Roy, 2017; Zhou et al., 2018) provide non-vacuous generalization guarantees. Specifically, they transform a base network into consequent networks that do not interpolate the training data either by adding stochasticity to the network weights (Dziugaite & Roy, 2017) or by compressing the original neural network (Zhou et al., 2018). In a similar spirit, our work provides guarantees on overparameterized networks by using early stopping or weight decay regularization, preventing a perfect fit on the training data. Notably, in our framework, the model can perfectly fit the clean portion of the data, so long as they nevertheless fit the mislabeled data poorly.

Leveraging noisy data to provide generalization guarantees In parallel work, Bansal et al. (2020) presented an upper bound on the generalization gap of linear classifiers trained on representations learned via self-supervision. Under certain noise-robustness and rationality assumptions on the training procedure, the authors obtained bounds dependent on the complexity of the linear classifier and independent of the complexity of representations. By contrast, we present generalization bounds for supervised learning that are non-vacuous by virtue of the early learning phenomenon. While both frameworks highlight how robustness to random label corruptions can be leveraged to obtain bounds that do not depend directly on the complexity of the underlying hypothesis class, our framework, methodology, claims, and generalization results are very different from theirs.

Other related work. A long line of work relates early stopped GD to a corresponding regularized solution (Friedman & Popescu, 2003; Yao et al., 2007; Suggala et al., 2018; Ali et al., 2018; Neu & Rosasco, 2018; Ali et al., 2020). In the most relevant work, Ali et al. (2018) and Suggala et al. (2018) address a regression task, theoretically relating the solutions of early-stopped GD and a regularized problem, obtained with a data-independent regularization coefficient. Towards understanding generalization numerous stability conditions have been discussed (Kearns & Ron, 1999; Bousquet & Elisseeff, 2002; Mukherjee et al., 2006; Shalev-Shwartz et al., 2010). Hardt et al. (2016) studies the uniform stability property to obtain generalization guarantees with early-stopped SGD. While we assume a benign stability condition to relate leave-one-out performance with population error, we do not rely on any stability condition that implies generalization.

B PROOFS SKETCH SEC. 2

We now present our proof sketches for ERM on the 0-1 loss (full proofs in App. C). We begin the discussion here with unregularized ERM. For any dataset T, ERM returns the classifier $\widehat{f}$ that minimizes the empirical error:

$$\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{T}}(f)\,, \tag{3}$$

To begin, we focus on binary classification with balanced classes. Assume we have a clean dataset $S \sim \mathcal{D}^n$ of n points and a randomly labeled dataset $\widetilde{S} \sim \widetilde{D}^m$ of $m(< n)$ points. Because the classes are balanced, labels in $\widetilde{S}$ are assigned uniformly at random. We show that with 0-1 loss minimization on the union of S and $\widetilde{S}$, we obtain a classifier whose population error (on $\mathcal{D}$) on the original data distribution is upper bounded by a function of the empirical errors on clean data $\mathcal{E}_{\mathcal{S}}$ (lower is better) and on randomly labeled data $\mathcal{E}_{\widetilde{\mathcal{S}}}$ (higher is better):

Theorem 4. *Assume we perform ERM as in* (3) *on $S \cup \widetilde{S}$ and obtain a classifier $\widehat{f}$. Then for any $\delta > 0$, with probability at least $1 - \delta$ we have*

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + 1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + \left(\sqrt{2}\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + 2 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}}\,. \tag{4}$$

Our proof strategy unfolds in three steps. First, in Lemma 1 we bound $\mathcal{E}_{\mathcal{D}}(\widehat{f})$ in terms of the error on the mislabeled subset of $\widetilde{S}$. Next, in Lemmas 2 and 3, we show that this quantity can be accurately estimated using only clean and randomly labeled data.

To begin, assume that we actually knew the original labels for the randomly labeled data. By $\widetilde{S}_C$ and $\widetilde{S}_M$, we denote the clean and mislabeled portions of the randomly labeled data, respectively (with $\widetilde{S} = \widetilde{S}_M \cup \widetilde{S}_C$). We refer to the distribution of mislabeled points as $\mathcal{D}'$. Note that for binary classification, a lower bound of the error on the mislabeled population $\mathcal{E}_{\mathcal{D}'}(\widehat{f})$ directly upper bounds the error on the original population $\mathcal{E}_{\mathcal{D}}(\widehat{f})$. Thus we need only to prove that the empirical error on the mislabeled portion of our data is lower than the error on unseen mislabeled data, i.e., $\mathcal{E}_{\widetilde{S}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f})$.

Lemma 1. *Assume the same setup as Theorem 4. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of mislabeled data $\widetilde{S}_M$, we have*

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant 1 - \mathcal{E}_{\widetilde{S}_M}(\widehat{f}) + \sqrt{\frac{\log(1/\delta)}{m}}\,. \tag{5}$$

Proof Sketch. The main idea of our proof is to regard the clean portion of the data ($S \cup \widetilde{S}_C$) as fixed. Then, there exists a classifier f^* that is optimal over draws of the mislabeled data $\widetilde{S}_M$, Formally, $f^* := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\breve{\mathcal{D}}}(f)$, where $\breve{\mathcal{D}}$ is a combination of the *empirical distribution* over correctly labeled data $S \cup \widetilde{S}_C$ and the (population) distribution over mislabeled data $\mathcal{D}'$. Recall that $\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f)$. Since, $\widehat{f}$ minimizes 0-1 error on $S \cup \widetilde{S}$, we have $\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f^*)$. Moreover, since f^* is independent of $\widetilde{S}_M$, we have with probability at least $1 - \delta$ that

$$\mathcal{E}_{\widetilde{S}_M}(f^*) \leqslant \mathcal{E}_{\mathcal{D}'}(f^*) + \sqrt{\frac{\log(1/\delta)}{m}}\,.$$

Finally, since f^* is the optimal classifier on $\breve{\mathcal{D}}$, we have $\mathcal{E}_{\breve{\mathcal{D}}}(f^*) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(\widehat{f})$. Combining the above steps and using the fact that $\mathcal{E}_{\mathcal{D}} = 1 - \mathcal{E}_{\mathcal{D}'}$, we obtain the desired result. □

While the LHS in (5) depends on the unknown portion $\widetilde{S}_M$, our goal is to use unlabeled data (with randomly assigned labels) for which the mislabeled portion cannot be readily identified. Fortunately, we do not need to identify the mislabeled points to estimate the error on these points in aggregate $\mathcal{E}_{\widetilde{S}_M}(\widehat{f})$. Note that because the label marginal is uniform, approximately half of the datapoints will be correctly labeled and the remaining half will be mislabeled. Consequently, we can utilize the value of $\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f})$ and an estimate of $\mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f})$ to lower bound $\mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f})$. We formalize this as follows:

Lemma 2. *Assume the same setup as Theorem 4. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of $\widetilde{S}$, we have* $\left|2\mathcal{E}_{\widetilde{S}}(\widehat{f}) - \mathcal{E}_{\widetilde{S}_C}(\widehat{f}) - \mathcal{E}_{\widetilde{S}_M}(\widehat{f})\right| \leqslant 2\mathcal{E}_{\widetilde{S}}(\widehat{f})\sqrt{\frac{\log(4/\delta)}{2m}}$.

To complete the argument, we show that due to the exchangeability of the clean data S and the clean portion of the randomly labeled data S_C, we can estimate the error on the latter $\mathcal{E}_{\widetilde{S}_C}(\widehat{f})$ by the error on the former $\mathcal{E}_{\mathcal{S}}(\widehat{f})$.

Lemma 3. *Assume the same setup as Theorem 4. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of $\widetilde{S}_C$ and S, we have* $\left|\mathcal{E}_{\widetilde{S}_C}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f})\right| \leqslant \left(1 + \frac{m}{2n}\right)\sqrt{\frac{\log(2/\delta)}{m}}$.

Lemma 3 establishes a tight bound on the difference of the error of classifier $\widehat{f}$ on $\widetilde{S}_C$ and on S. The proof uses Hoeffding's inequality for randomly sampled points from a fixed population (Hoeffding, 1994; Bardenet et al., 2015).

Having established these core components, we can now summarize the proof strategy for Theorem 4. We bound the population error on clean data (the term in LHS in Theorem 4) in three steps: (i) use Lemma 1 to upper bound the error on clean distribution $\mathcal{E}_{\mathcal{D}}(\widehat{f})$, by the error on mislabeled training data $\mathcal{E}_{\widetilde{S}_M}(\widehat{f})$; (ii) approximate $\mathcal{E}_{\widetilde{S}_M}(\widehat{f})$ by $\mathcal{E}_{\widetilde{S}_C}(\widehat{f})$ and the error on randomly labeled training data (i.e., $\mathcal{E}_{\widetilde{S}}(\widehat{f})$) using Lemma 2; and (iii) use Lemma 3 to estimate $\mathcal{E}_{\widetilde{S}_C}(\widehat{f})$ using the error on clean training data ($\mathcal{E}_{\mathcal{S}}(\widehat{f})$).

Extension to multiclass classification The core of our proof involves obtaining an inequality similar to (5). While for binary classification, we could upper bound $\mathcal{E}_{\widetilde{S}_M}$ with $1 - \mathcal{E}_{\mathcal{D}}$ (in the proof of Lemma 1), for multiclass classification, error on the mislabeled data and accuracy on the clean data in the population are not so directly related. To establish an inequality analogous to (5), we break the error on the (unknown) mislabeled data into two parts: one term corresponds to predicting the true label on mislabeled data, and the other corresponds to predicting neither the true label nor the assigned (mis-)label. Finally, we relate these errors to their population counterparts to establish an inequality similar to (5).

C Proofs from Sec. 2

Throughout this discussion, we will make frequently use of the following standard results concerning the exponential concentration of random variables:

Lemma 4 (Hoeffding's inequality for independent RVs (Hoeffding, 1994))**.** *Let $Z_1, Z_2, \ldots, Z_n$ be independent bounded random variables with $Z_i \in [a, b]$ for all i, then*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}(Z_i - \mathbb{E}\left[Z_i\right]) \geqslant t\right) \leqslant \exp\left(-\frac{2nt^2}{(b-a)^2}\right)$$

and

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}(Z_i - \mathbb{E}\left[Z_i\right]) \leqslant -t\right) \leqslant \exp\left(-\frac{2nt^2}{(b-a)^2}\right)$$

for all $t \geqslant 0$.

Lemma 5 (Hoeffding's inequality for sampling with replacement (Hoeffding, 1994))**.** *Let $\mathcal{Z} = (Z_1, Z_2, \ldots, Z_N)$ be a finite population of N points with $Z_i \in [a.b]$ for all i. Let $X_1, X_2, \ldots X_n$ be a random sample drawn without replacement from $\mathcal{Z}$. Then for all $t \geqslant 0$, we have*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}(X_i - \mu) \geqslant t\right) \leqslant \exp\left(-\frac{2nt^2}{(b-a)^2}\right)$$

and

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n}(X_i - \mu) \leqslant -t\right) \leqslant \exp\left(-\frac{2nt^2}{(b-a)^2}\right),$$

where $\mu = \frac{1}{N}\sum_{i=1}^{N} Z_i$.

We now discuss one condition that generalizes the exponential concentration to dependent random variables.

Condition 2 (Bounded difference inequality)**.** *Let $\mathcal{Z}$ be some set and $\phi : \mathcal{Z}^n \to \mathbb{R}$. We say that ϕ satisfies the bounded difference assumption if there exists $c_1, c_2, \dots c_n \geqslant 0$ s.t. for all i, we have*

$$\sup_{Z_1, Z_2, \dots, Z_n, Z_i' \in \mathcal{Z}^{n+1}} \left|\phi(Z_1, \dots, Z_i, \dots, Z_n) - \phi(Z_1, \dots, Z_i', \dots, Z_n)\right| \leqslant c_i \,.$$

Lemma 6 (McDiarmid's inequality (McDiarmid, 1989))**.** *Let $Z_1, Z_2, \dots, Z_n$ be independent random variables on set $\mathcal{Z}$ and $\phi : \mathcal{Z}^n \to \mathbb{R}$ satisfy bounded difference inequality (Condition 2). Then for all $t > 0$, we have*

$$\mathbb{P}\left(\phi(Z_1, Z_2, \dots, Z_n) - \mathbb{E}\left[\phi(Z_1, Z_2, \dots, Z_n)\right] \geqslant t\right) \leqslant \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right)$$

and

$$\mathbb{P}\left(\phi(Z_1, Z_2, \dots, Z_n) - \mathbb{E}\left[\phi(Z_1, Z_2, \dots, Z_n)\right] \leqslant -t\right) \leqslant \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right)$$

Additional notation By $\|\cdot\|$, and $\langle \cdot, \cdot \rangle$ we denote the Euclidean norm and inner product, respectively. For a vector $v \in \mathbb{R}^d$, we use v_j to denote its j^{th} entry, and for an event E we let $\mathbb{I}\left[E\right]$ denote the binary indicator of the event. Let m_1 be the number of mislabeled points ($\widetilde{S}_M$) and m_2 be the number of correctly labeled points ($\widetilde{S}_C$). Note $m_1 + m_2 = m$.

C.1 Proof of Theorem 4

Proof of Lemma 1. The main idea of our proof is to regard the clean portion of the data ($S \cup \widetilde{S}_C$) as fixed. Then, there exists an (unknown) classifier f^* that minimizes the expected risk calculated on the (fixed) clean data and (random draws of) the mislabeled data $\widetilde{S}_M$. Formally,

$$f^* := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\breve{\mathcal{D}}}(f) \,, \tag{6}$$

where

$$\breve{\mathcal{D}} = \frac{n}{m+n}\mathcal{S} + \frac{m_2}{m+n}\widetilde{\mathcal{S}}_C + \frac{m_1}{m+n}\mathcal{D}' \,.$$

Note here that $\breve{\mathcal{D}}$ is a combination of the *empirical distribution* over correctly labeled data $S \cup \widetilde{S}_C$ and the (population) distribution over mislabeled data $\mathcal{D}'$. Recall that

$$\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f) \,. \tag{7}$$

Since, $\widehat{f}$ minimizes 0-1 error on $S \cup \widetilde{S}$, using ERM optimality on (7), we have

$$\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f^*) \,. \tag{8}$$

Moreover, since f^* is independent of $\widetilde{S}_M$, using Hoeffding's bound, we have with probability at least $1 - \delta$ that

$$\mathcal{E}_{\widetilde{\mathcal{S}}_M}(f^*) \leqslant \mathcal{E}_{\mathcal{D}'}(f^*) + \sqrt{\frac{\log(1/\delta)}{2m_1}} \,. \tag{9}$$

Finally, since f^* is the optimal classifier on $\breve{\mathcal{D}}$, we have

$$\mathcal{E}_{\breve{\mathcal{D}}}(f^*) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(\widehat{f}) \tag{10}$$

Now to relate (8) and (10), we multiply (9) by $\frac{m_1}{m+n}$ and add $\frac{n}{m+n}\mathcal{E}_{\mathcal{S}}(f) + \frac{m_2}{m+n}\mathcal{E}_{\widetilde{\mathcal{S}}_C}(f)$ both the sides. Hence, we can rewrite (9) as follows:

$$\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f^*) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(f^*) + \frac{m_1}{m+n}\sqrt{\frac{\log(1/\delta)}{2m_1}} \,. \tag{11}$$

Now we combine equations (8), (11), and (10), to get

$$\mathcal{E}_{\mathcal{S}\cup\tilde{\mathcal{S}}}(\widehat{f}) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(\widehat{f}) + \frac{m_1}{m+n}\sqrt{\frac{\log(1/\delta)}{2m_1}}\,, \tag{12}$$

which implies

$$\mathcal{E}_{\tilde{\mathcal{S}}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f}) + \sqrt{\frac{\log(1/\delta)}{2m_1}}\,. \tag{13}$$

Since $\widetilde{S}$ is obtained by randomly labeling an unlabeled dataset, we assume $2m_1 \approx m$ [1]. Moreover, using $\mathcal{E}_{\mathcal{D}'} = 1 - \mathcal{E}_{\mathcal{D}}$ we obtain the desired result. □

Proof of Lemma 2. Recall $\mathcal{E}_{\widetilde{S}}(f) = \frac{m_1}{m}\mathcal{E}_{\widetilde{S}_M}(f) + \frac{m_2}{m}\mathcal{E}_{\widetilde{S}_C}(f)$. Hence, we have

$$2\mathcal{E}_{\widetilde{S}}(f) - \mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_C}(f) = \left(\frac{2m_1}{m}\mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_M}(f)\right) + \left(\frac{2m_2}{m}\mathcal{E}_{\widetilde{S}_C}(f) - \mathcal{E}_{\widetilde{S}_C}(f)\right) \tag{14}$$

$$= \left(\frac{2m_1}{m} - 1\right)\mathcal{E}_{\widetilde{S}_M}(f) + \left(\frac{2m_2}{m} - 1\right)\mathcal{E}_{\widetilde{S}_C}(f)\,. \tag{15}$$

Since the dataset is randomly labeled, with probability at least $1-\delta$, we have $\left(\frac{2m_1}{m} - 1\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m}}$. Similarly, we have with probability at least $1-\delta$, $\left(\frac{2m_2}{m} - 1\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m}}$. Using union bound, we have with probability at least $1-\delta$

$$2\mathcal{E}_{\widetilde{S}} - \mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_C}(f) \leqslant \sqrt{\frac{\log(2/\delta)}{2m}}\left(\mathcal{E}_{\widetilde{S}_M}(f) + \mathcal{E}_{\widetilde{S}_C}(f)\right)\,. \tag{16}$$

With re-arranging $\mathcal{E}_{\widetilde{S}_M}(f) + \mathcal{E}_{\widetilde{S}_C}(f)$ and using the inequality $1 - a \leqslant \frac{1}{1+a}$, we have

$$2\mathcal{E}_{\widetilde{S}} - \mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_C}(f) \leqslant 2\mathcal{E}_{\widetilde{S}}\sqrt{\frac{\log(2/\delta)}{2m}}\,. \tag{17}$$

□

Proof of Lemma 3. In the set of correctly labeled points $S \cup \widetilde{S}_C$, we have S as a random subset of $S \cup \widetilde{S}_C$. Hence, using Hoeffding's inequality for sampling without replacement (Lemma 5), we have with probability at least $1-\delta$

$$\mathcal{E}_{\tilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}\cup\tilde{\mathcal{S}}_C}(\widehat{f}) \leqslant \sqrt{\frac{\log(1/\delta)}{2m_2}}\,. \tag{18}$$

Re-writing $\mathcal{E}_{\mathcal{S}\cup\tilde{\mathcal{S}}_C}(\widehat{f})$ as $\frac{m_2}{m_2+n}\mathcal{E}_{\tilde{\mathcal{S}}_C}(\widehat{f}) + \frac{n}{m_2+n}\mathcal{E}_{\mathcal{S}}(\widehat{f})$, we have with probability at least $1-\delta$

$$\left(\frac{n}{n+m_2}\right)\left(\mathcal{E}_{\tilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f})\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m_2}}\,. \tag{19}$$

As before, assuming $2m_2 \approx m$, we have with probability at least $1-\delta$

$$\mathcal{E}_{\tilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f}) \leqslant \left(1 + \frac{m_2}{n}\right)\sqrt{\frac{\log(1/\delta)}{m}} \leqslant \left(1 + \frac{m}{2n}\right)\sqrt{\frac{\log(1/\delta)}{m}}\,. \tag{20}$$

□

Proof of Theorem 4. Having established these core intermediate results, we can now combine above three lemmas to prove the main result. In particular, we bound the population error on clean data ($\mathcal{E}_{\mathcal{D}}(\widehat{f})$) as follows:

[1] Formally, with probability at least $1-\delta$, we have $(m - 2m_1) \leqslant \sqrt{m\log(1/\delta)/2}$

(i) First, use (13), to obtain an upper bound on the population error on clean data, i.e., with probability at least $1 - \delta/4$, we have

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant 1 - \mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f}) + \sqrt{\frac{\log(4/\delta)}{m}}\,. \tag{21}$$

(ii) Second, use (17), to relate the error on the mislabeled fraction with error on clean portion of randomly labeled data and error on whole randomly labeled dataset, i.e., with probability at least $1 - \delta/2$, we have

$$-\mathcal{E}_{\widetilde{S}_M}(f) \leqslant \mathcal{E}_{\widetilde{S}_C}(f) - 2\mathcal{E}_{\widetilde{S}} + 2\mathcal{E}_{\widetilde{S}}\sqrt{\frac{\log(4/\delta)}{2m}}\,. \tag{22}$$

(iii) Finally, use (20) to relate the error on the clean portion of randomly labeled data and error on clean training data, i.e., with probability $1 - \delta/4$, we have

$$\mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f}) \leqslant -\mathcal{E}_{\mathcal{S}}(\widehat{f}) + \left(1 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}}\,. \tag{23}$$

Using union bound on the above three steps, we have with probability at least $1 - \delta$:

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + 1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + \left(\sqrt{2}\mathcal{E}_{\widetilde{S}} + 2 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}}\,. \tag{24}$$

□

C.2 Proof of Proposition 1

Proof of Proposition 1. For a classifier $f : \mathcal{X} \to \{-1, 1\}$, we have $1 - 2\,\mathbb{I}\left[f(x) \neq y\right] = y \cdot f(x)$. Hence, by definition of $\mathcal{E}$, we have

$$1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(f) = \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i) \leqslant \sup_{f\in\mathcal{F}} \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i)\,. \tag{25}$$

Note that for fixed inputs $(x_1, x_2, \ldots, x_m)$ in $\widetilde{S}$, $(y_1, y_2, \ldots y_m)$ are random labels. Define $\phi_1(y_1, y_2, \ldots, y_m) := \sup_{f\in\mathcal{F}} \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i)$. We have the following bounded difference condition on ϕ_1. For all i,

$$\sup_{y_1,\ldots y_m, y_i'\in\{-1,1\}^{m+1}} \left|\phi_1(y_1, \ldots, y_i, \ldots, y_m) - \phi_1(y_1, \ldots, y_i', \ldots, y_m)\right| \leqslant 1/m\,. \tag{26}$$

Similarly, we define $\phi_2(x_1, x_2, \ldots, x_m) := \mathbb{E}_{y_i\sim U\{-1,1\}}\left[\sup_{f\in\mathcal{F}} \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i)\right]$. We have the following bounded difference condition on ϕ_2. For all i,

$$\sup_{x_1,\ldots x_m, x_i'\in\mathcal{X}^{m+1}} \left|\phi_2(x_1, \ldots, x_i, \ldots, x_m) - \phi_1(x_1, \ldots, x_i', \ldots, x_m)\right| \leqslant 1/m\,. \tag{27}$$

Using McDiarmid's inequality (Lemma 6) twice with Condition (26) and (27), with probability at least $1 - \delta$, we have

$$\sup_{f\in\mathcal{F}} \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i) - \mathbb{E}_{x,y}\left[\sup_{f\in\mathcal{F}} \frac{1}{m}\sum_{i=1}^{m} y_i \cdot f(x_i)\right] \leqslant \sqrt{\frac{2\log(2/\delta)}{m}} \tag{28}$$

Combining (25) and (28), we obtain the desired result. □

C.3 Proof of Theorem 1

Proof of Theorem 1 follows similar to the proof of Theorem 4. Note that the same results in Lemma 1, Lemma 2, and Lemma 3 hold in the regularized ERM case. However, the arguments in the proof of Lemma 1 changes slightly. Hence, we state and prove a lemma parallel to Lemma 1 for completeness.

Lemma 7. *Assume the same setup as Theorem 1. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of mislabeled data $\widetilde{S}_M$, we have*

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant 1 - \mathcal{E}_{\widetilde{S}_M}(\widehat{f}) + \sqrt{\frac{\log(1/\delta)}{m}}\,. \tag{29}$$

Proof. The main idea of the proof remains the same, i.e. regard the clean portion of the data ($S \cup \widetilde{S}_C$) as fixed. Then, there exists a classifier f^* that is optimal over draws of the mislabeled data $\widetilde{S}_M$.

Formally,

$$f^* := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\breve{\mathcal{D}}}(f) + \lambda R(f)\,, \tag{30}$$

where

$$\breve{\mathcal{D}} = \frac{n}{m+n}\mathcal{S} + \frac{m_1}{m+n}\widetilde{\mathcal{S}}_C + \frac{m_2}{m+n}\mathcal{D}'\,.$$

That is, $\breve{\mathcal{D}}$ a combination of the *empirical distribution* over correctly labeled data $S \cup \widetilde{S}_C$ and the (population) distribution over mislabeled data $\mathcal{D}'$. Recall that

$$\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{S} \cup \widetilde{S}}(f) + \lambda R(f)\,. \tag{31}$$

Since, $\widehat{f}$ minimizes 0-1 error on $S \cup \widetilde{S}$, using ERM optimality on (7), we have

$$\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(\widehat{f}) + \lambda R(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f^*) + \lambda R(f^*)\,. \tag{32}$$

Moreover, since f^* is independent of $\widetilde{S}_M$, using Hoeffding's bound, we have with probability at least $1 - \delta$ that

$$\mathcal{E}_{\widetilde{\mathcal{S}}_M}(f^*) \leqslant \mathcal{E}_{\mathcal{D}'}(f^*) + \sqrt{\frac{\log(1/\delta)}{2m_1}}\,. \tag{33}$$

Finally, since f^* is the optimal classifier on $\breve{\mathcal{D}}$, we have

$$\mathcal{E}_{\breve{\mathcal{D}}}(f^*) + \lambda R(f^*) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(\widehat{f}) + \lambda R(\widehat{f}) \tag{34}$$

Now to relate (32) and (34), we can re-write the (33) as follows:

$$\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f^*) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(f^*) + \frac{m_1}{m+n}\sqrt{\frac{\log(1/\delta)}{2m_1}}\,. \tag{35}$$

After adding $\lambda R(f^*)$ on both sides in (35), we combine equations (32), (35), and (34), to get

$$\mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(\widehat{f}) \leqslant \mathcal{E}_{\breve{\mathcal{D}}}(\widehat{f}) + \frac{m_1}{m+n}\sqrt{\frac{\log(1/\delta)}{2m_1}}\,, \tag{36}$$

which implies

$$\mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f}) + \sqrt{\frac{\log(1/\delta)}{2m_1}}\,. \tag{37}$$

Similar as before, since $\widetilde{S}$ is obtained by randomly labeling an unlabeled dataset, we assume $2m_1 \approx m$. Moreover, using $\mathcal{E}_{\mathcal{D}'} = 1 - \mathcal{E}_{\mathcal{D}}$ we obtain the desired result. □

C.4 Proof of Theorem 2

To prove our results in the multiclass case, we first state and prove lemmas parallel to those used in the proof of balanced binary case. We then combine these results to obtain the result in Theorem 2.

Before stating the result, we define mislabeled distribution $\mathcal{D}'$ for any $\mathcal{D}$. While $\mathcal{D}'$ and $\mathcal{D}$ share the same marginal distribution over inputs $\mathcal{X}$, the conditional distribution over labels y given an input $x \sim \mathcal{D}_{\mathcal{X}}$ is changed as follows: For any x, the pdf over y is changed to: $p_{\mathcal{D}'}(\cdot|x) := \frac{1 - p_{\mathcal{D}}(\cdot|x)}{k-1}$.

Lemma 8. *Assume the same setup as Theorem 2. Then for any $\delta > 0$, with probability at least $1 - \delta$ over the random draws of mislabeled data $\widetilde{S}_M$, we have*

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant (k-1)\left(1 - \mathcal{E}_{\widetilde{S}_M}(\widehat{f})\right) + (k-1)\sqrt{\frac{\log(1/\delta)}{m}}\,. \tag{38}$$

Proof. The main idea of the proof remains the same. We begin by regarding the clean portion of the data ($S \cup \widetilde{S}_C$) as fixed. Then, there exists a classifier f^* that is optimal over draws of the mislabeled data $\widetilde{S}_M$.

However, in the multiclass case, we cannot as easily relate the population error on mislabeled data to the population accuracy on clean data. While for binary classification, we could lower bound the population accuracy $1 - \mathcal{E}_{\mathcal{D}}$ with the empirical error on mislabeled data $\mathcal{E}_{\widetilde{S}_M}$ (in the proof of Lemma 1), for multiclass classification, error on the mislabeled data and accuracy on the clean data in the population are not so directly related. To establish (38), we break the error on the (unknown) mislabeled data into two parts: one term corresponds to predicting the true label on mislabeled data, and the other corresponds to predicting neither the true label nor the assigned (mis-)label. Finally, we relate these errors to their population counterparts to establish (38).

Formally,

$$f^* := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\breve{\mathcal{D}}}(f) + \lambda R(f)\,, \tag{39}$$

where

$$\breve{\mathcal{D}} = \frac{n}{m+n}\mathcal{S} + \frac{m_1}{m+n}\widetilde{\mathcal{S}}_C + \frac{m_2}{m+n}\mathcal{D}'\,.$$

That is, $\breve{\mathcal{D}}$ is a combination of the *empirical distribution* over correctly labeled data $S \cup \widetilde{S}_C$ and the (population) distribution over mislabeled data $\mathcal{D}'$. Recall that

$$\widehat{f} := \arg\min_{f \in \mathcal{F}} \mathcal{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}}(f) + \lambda R(f)\,. \tag{40}$$

Following the exact steps from the proof of Lemma 7, with probability at least $1 - \delta$, we have

$$\mathcal{E}_{\widetilde{S}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f}) + \sqrt{\frac{\log(1/\delta)}{2m_1}}\,. \tag{41}$$

Similar to before, since $\widetilde{S}$ is obtained by randomly labeling an unlabeled dataset, we assume $\frac{k}{k-1}m_1 \approx m$.

Now we will relate $\mathcal{E}'_{\mathcal{D}}(\widehat{f})$ with $\mathcal{E}_{\mathcal{D}}(\widehat{f})$. Let y^T denote the (unknown) true label for a mislabeled point (x, y) (i.e., label before replacing it with a mislabel).

$$\begin{aligned}\mathbb{E}_{(x,y)\in\sim\mathcal{D}'}\left[\mathbb{I}\left[\widehat{f}(x) \neq y\right]\right] = \underbrace{\mathbb{E}_{(x,y)\in\sim\mathcal{D}'}\left[\mathbb{I}\left[\widehat{f}(x) \neq y \wedge \widehat{f}(x) \neq y^T\right]\right]}_{\text{I}} \\ + \underbrace{\mathbb{E}_{(x,y)\in\sim\mathcal{D}'}\left[\mathbb{I}\left[\widehat{f}(x) \neq y \wedge \widehat{f}(x) = y^T\right]\right]}_{\text{II}}\,.\end{aligned} \tag{42}$$

Clearly, term 2 is one minus the accuracy on the clean unseen data, i.e.,

$$\text{II} = 1 - \mathbb{E}_{x,y\sim\mathcal{D}}\left[\mathbb{I}\left[\widehat{f}(x) \neq y\right]\right] = 1 - \mathcal{E}_{\mathcal{D}}(\widehat{f})\,. \tag{43}$$

Next, we relate term 1 with the error on the unseen clean data. We show that term 1 is equal to the error on the unseen clean data scaled by $\frac{k-2}{k-1}$, where k is the number of labels. Using the definition of mislabeled distribution $\mathcal{D}'$, we have

$$\text{I} = \frac{1}{k-1}\left(\mathbb{E}_{(x,y)\in\sim\mathcal{D}}\left[\sum_{i\in\mathcal{Y}\wedge i\neq y}\mathbb{I}\left[\widehat{f}(x) \neq i \wedge \widehat{f}(x) \neq y\right]\right]\right) = \frac{k-2}{k-1}\mathcal{E}_{\mathcal{D}}(\widehat{f})\,. \tag{44}$$

Combining the result in (43), (44) and (42), we have

$$\mathcal{E}_{\mathcal{D}'}(\widehat{f}) = 1 - \frac{1}{k-1}\mathcal{E}_{\mathcal{D}}(\widehat{f})\,. \tag{45}$$

Finally, combining the result in (45) with equation (41), we have with probability $1-\delta$,

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant (k-1)\left(1 - \mathcal{E}_{\widetilde{S}_M}(\widehat{f})\right) + (k-1)\sqrt{\frac{k\log(1/\delta)}{2(k-1)m}}\,. \tag{46}$$

□

Lemma 9. *Assume the same setup as Theorem 2. Then for any $\delta > 0$, with probability at least $1-\delta$ over the random draws of $\widetilde{S}$, we have*

$$\left|k\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) - \mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f}) - (k-1)\mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f})\right| \leqslant 2k\sqrt{\frac{\log(4/\delta)}{2m}}\,.$$

Proof. Recall $\mathcal{E}_{\widetilde{S}}(f) = \frac{m_1}{m}\mathcal{E}_{\widetilde{S}_M}(f) + \frac{m_2}{m}\mathcal{E}_{\widetilde{S}_C}(f)$. Hence, we have

$$\begin{aligned} k\mathcal{E}_{\widetilde{S}}(f) - (k-1)\mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_C}(f) &= (k-1)\left(\frac{km_1}{(k-1)m}\mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_M}(f)\right) \\ &\quad + \left(\frac{km_2}{m}\mathcal{E}_{\widetilde{S}_C}(f) - \mathcal{E}_{\widetilde{S}_C}(f)\right) \qquad (47) \\ &= k\left[\left(\frac{m_1}{m} - \frac{k-1}{k}\right)\mathcal{E}_{\widetilde{S}_M}(f) + \left(\frac{m_2}{m} - \frac{1}{k}\right)\mathcal{E}_{\widetilde{S}_C}(f)\right]. \qquad (48) \end{aligned}$$

Since the dataset is randomly labeled, we have with probability at least $1-\delta$, $\left(\frac{m_1}{m} - \frac{k-1}{k}\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m}}$. Similarly, we have with probability at least $1-\delta$, $\left(\frac{m_2}{m} - \frac{1}{k}\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m}}$. Using union bound, we have with probability at least $1-\delta$

$$k\mathcal{E}_{\widetilde{S}}(f) - (k-1)\mathcal{E}_{\widetilde{S}_M}(f) - \mathcal{E}_{\widetilde{S}_C}(f) \leqslant k\sqrt{\frac{\log(2/\delta)}{2m}}\left(\mathcal{E}_{\widetilde{S}_M}(f) + \mathcal{E}_{\widetilde{S}_C}(f)\right). \tag{49}$$

□

Lemma 10. *Assume the same setup as Theorem 2. Then for any $\delta > 0$, with probability at least $1-\delta$ over the random draws of $\widetilde{S}_C$ and S, we have*

$$\left|\mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f})\right| \leqslant 1.5\sqrt{\frac{k\log(2/\delta)}{2m}}\,.$$

Proof. In the set of correctly labeled points $S \cup \widetilde{S}_C$, we have S as a random subset of $S \cup \widetilde{S}_C$. Hence, using Hoeffding's inequality for sampling without replacement (Lemma 5), we have with probability at least $1-\delta$

$$\mathcal{E}_{\widetilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}\cup\widetilde{\mathcal{S}}_C}(\widehat{f}) \leqslant \sqrt{\frac{\log(1/\delta)}{2m_2}}\,. \tag{50}$$

Re-writing $\mathcal{E}_{\mathcal{S}\cup\widetilde{\mathcal{S}}_C}(\widehat{f})$ as $\frac{m_2}{m_2+n}\mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f}) + \frac{n}{m_2+n}\mathcal{E}_{\mathcal{S}}(\widehat{f})$, we have with probability at least $1-\delta$

$$\left(\frac{n}{n+m_2}\right)\left(\mathcal{E}_{\widetilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f})\right) \leqslant \sqrt{\frac{\log(1/\delta)}{2m_2}}\,. \tag{51}$$

As before, assuming $km_2 \approx m$, we have with probability at least $1-\delta$

$$\mathcal{E}_{\widetilde{\mathcal{S}}_c}(\widehat{f}) - \mathcal{E}_{\mathcal{S}}(\widehat{f}) \leqslant \left(1 + \frac{m_2}{n}\right)\sqrt{\frac{k\log(1/\delta)}{2m}} \leqslant \left(1 + \frac{1}{k}\right)\sqrt{\frac{k\log(1/\delta)}{2m}}\,. \tag{52}$$

□

Proof of Theorem 2. Having established these core intermediate results, we can now combine above three lemmas. In particular, we bound the population error on clean data ($\mathcal{E}_{\mathcal{D}}(\widehat{f})$) as follows:

(i) First, use (46), to obtain an upper bound on the population error on clean data, i.e., with probability at least $1 - \delta/4$, we have

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant (k-1)\left(1 - \mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f})\right) + (k-1)\sqrt{\frac{k\log(4/\delta)}{2(k-1)m}}\,. \tag{53}$$

(ii) Second, use (49) to relate the error on the mislabeled fraction with error on clean portion of randomly labeled data and error on whole randomly labeled dataset, i.e., with probability at least $1 - \delta/2$, we have

$$-(k-1)\mathcal{E}_{\widetilde{S}_M}(f) \leqslant \mathcal{E}_{\widetilde{S}_C}(f) - k\mathcal{E}_{\widetilde{S}} + k\sqrt{\frac{\log(4/\delta)}{2m}}\,. \tag{54}$$

(iii) Finally, use (52) to relate the error on the clean portion of randomly labeled data and error on clean training data, i.e., with probability $1 - \delta/4$, we have

$$\mathcal{E}_{\widetilde{\mathcal{S}}_C}(\widehat{f}) \leqslant -\mathcal{E}_{\mathcal{S}}(\widehat{f}) + \left(1 + \frac{m}{kn}\right)\sqrt{\frac{k\log(4/\delta)}{2m}}\,. \tag{55}$$

Using union bound on the above three steps, we have with probability at least $1 - \delta$:

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + (k-1) - k\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + (\sqrt{k(k-1)} + k + \sqrt{k} + \frac{m}{n\sqrt{k}})\sqrt{\frac{\log(4/\delta)}{2m}}\,. \tag{56}$$

Simplifying the term in RHS of (56), we get the desired result. in the final bound. □

D PROOFS AND ADDITIONAL RESULTS FOR LINEAR MODELS WITH GD TRAINING

We suppose that the parameters of the linear function are obtained via gradient descent on the following L_2 regularized problem:

$$\mathcal{L}_S(w;\lambda) := \sum_{i=1}^{n} (w^T x_i - y_i)^2 + \lambda \|w\|_2^2 \,, \tag{57}$$

where $\lambda \geqslant 0$ is a regularization parameter. We assume access to a clean dataset $S = \{(x_i, y_i)\}_{i=1}^n \sim \mathcal{D}^n$ and randomly labeled dataset $\widetilde{S} = \{(x_i, y_i)\}_{i=n+1}^{n+m} \sim \widetilde{\mathcal{D}}^m$. Let $\boldsymbol{X} = [x_1, x_2, \cdots, x_{m+n}]$ and $\boldsymbol{y} = [y_1, y_2, \cdots, y_{m+n}]$. Fix a positive learning rate η such that $\eta \leqslant 1/\left(\left\|\boldsymbol{X}^T\boldsymbol{X}\right\|_{\text{op}} + \lambda^2\right)$ and an initialization $w_0 = 0$. Consider the following gradient descent iterates to minimize objective (57) on $S \cup \widetilde{S}$:

$$w_t = w_{t-1} - \eta \nabla_w \mathcal{L}_{S\cup\widetilde{S}}(w_{t-1};\lambda) \quad \forall t = 1, 2, \ldots \tag{58}$$

Then we have $\{w_t\}$ converge to the limiting solution $\widehat{w} = \left(\boldsymbol{X}^T\boldsymbol{X} + \lambda \boldsymbol{I}\right)^{-1} \boldsymbol{X}^T \boldsymbol{y}$. Define $\widehat{f}(x) := f(x;\widehat{w})$.

D.1 PROOF OF THEOREM 3

We use a standard result from linear algebra, namely the Shermann-Morrison formula (Sherman & Morrison, 1950) for matrix inversion:

Lemma 11 (Sherman & Morrison (1950))**.** *Suppose $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ is an invertible square matrix and $u, v \in \mathbb{R}^n$ are column vectors. Then $\boldsymbol{A} + uv^T$ is invertible iff $1 + v^T\boldsymbol{A}u \neq 0$ and in particular*

$$(\boldsymbol{A} + uv^T)^{-1} = \boldsymbol{A}^{-1} - \frac{\boldsymbol{A}^{-1}uv^T\boldsymbol{A}^{-1}}{1 + v^T\boldsymbol{A}^{-1}u} \,. \tag{59}$$

For a given training set $S \cup \widetilde{S}_C$, define leave-one-out error on mislabeled points in the training data as

$$\mathcal{E}_{\text{LOO}(\widetilde{S}_M)} = \frac{\sum_{(x_i,y_i)\in\widetilde{S}_M} \mathcal{E}(f_{(i)}(x_i), y_i)}{\left|\widetilde{S}_M\right|} \,,$$

where $f_{(i)} := f(\mathcal{A}, (S \cup \widetilde{S})_{(i)})$. To relate empirical leave-one-out error and population error with hypothesis stability condition, we use the following lemma:

Lemma 12 (Bousquet & Elisseeff (2002))**.** *For the leave-one-out error, we have*

$$\mathbb{E}\left[\left(\mathcal{E}_{\mathcal{D}'}(\widehat{f}) - \mathcal{E}_{LOO(\widetilde{S}_M)}\right)^2\right] \leqslant \frac{1}{2m_1} + \frac{3\beta}{n+m} \,. \tag{60}$$

Proof of the above lemma is similar to the proof of Lemma 9 in Bousquet & Elisseeff (2002) and can be found in App. F. Before presenting the proof of Theorem 3, we introduce some more notation. Let $\boldsymbol{X}_{(i)}$ denote the matrix of covariates with the i^{th} point removed. Similarly, let $\boldsymbol{y}_{(i)}$ be the array of responses with the i^{th} point removed. Define the corresponding regularized GD solution as $\widehat{w}_{(i)} = \left(\boldsymbol{X}_{(i)}^T\boldsymbol{X}_{(i)} + \lambda\boldsymbol{I}\right)^{-1}\boldsymbol{X}_{(i)}^T\boldsymbol{y}_{(i)}$. Define $\widehat{f}_{(i)}(x) := f(x;\widehat{w}_{(i)})$.

Proof of Theorem 3. Because squared loss minimization does not imply 0-1 error minimization, we cannot use arguments from Lemma 1. This is the main technical difficulty. To compare the 0-1 error at a train point with an unseen point, we use the closed-form expression for $\widehat{w}$ and Shermann-Morrison formula to upper bound training error with leave-one-out cross validation error.

The proof is divided into three parts: In part one, we show that 0-1 error on mislabeled points in the training set is lower than the error obtained by leave-one-out error at those points. In part two, we relate this leave-one-out error with the population error on mislabeled distribution using Condition 1.

While the empirical leave-one-out error is an unbiased estimator of the average population error of leave-one-out classifiers, we need hypothesis stability to control the variance of empirical leave-one-out error. Finally, in part three, we show that the error on the mislabeled training points can be estimated with just the randomly labeled and clean training data (as in proof of Theorem 4).

Part 1 First we relate training error with leave-one-out error. For any training point (x_i, y_i) in $\widetilde{S} \cup S$, we have

$$\mathcal{E}(\widehat{f}(x_i), y_i) = \mathbb{I}\left[y_i \cdot x_i^T \widehat{w} < 0\right] = \mathbb{I}\left[y_i \cdot x_i^T \left(\boldsymbol{X}^T \boldsymbol{X} + \lambda \boldsymbol{I}\right)^{-1} \boldsymbol{X}^T \boldsymbol{y} < 0\right] \tag{61}$$

$$= \mathbb{I}\left[y_i \cdot x_i^T \underbrace{\left(\boldsymbol{X}_{(i)}^T \boldsymbol{X}_{(i)} + x_i^T x_i + \lambda \boldsymbol{I}\right)^{-1}}_{\mathrm{I}} (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)} + y \cdot x_i) < 0 \right] \tag{62}$$

Letting $\boldsymbol{A} = \left(\boldsymbol{X}_{(i)}^T \boldsymbol{X}_{(i)} + \lambda \boldsymbol{I}\right)$ and using Lemma 11 on term 1, we have

$$\mathcal{E}(\widehat{f}(x_i), y_i) = \mathbb{I}\left[y_i \cdot x_i^T \left[\boldsymbol{A}^{-1} - \frac{\boldsymbol{A}^{-1} x_i x_i^T \boldsymbol{A}^{-1}}{1 + x_i^T \boldsymbol{A}^{-1} x_i} \right] (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)} + y \cdot x_i) < 0 \right] \tag{63}$$

$$= \mathbb{I}\left[y_i \cdot \left[\frac{x_i^T \boldsymbol{A}^{-1}(1 + x_i^T \boldsymbol{A}^{-1} x_i) - x_i^T \boldsymbol{A}^{-1} x_i x_i^T \boldsymbol{A}^{-1}}{1 + x_i^T \boldsymbol{A}^{-1} x_i} \right] (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)} + y \cdot x_i) < 0 \right] \tag{64}$$

$$= \mathbb{I}\left[y_i \cdot \left[\frac{x_i^T \boldsymbol{A}^{-1}}{1 + x_i^T \boldsymbol{A}^{-1} x_i} \right] (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)} + y \cdot x_i) < 0 \right]. \tag{65}$$

Since $1 + x_i^T \boldsymbol{A}^{-1} x_i > 0$, we have

$$\mathcal{E}(\widehat{f}(x_i), y_i) = \mathbb{I}\left[y_i \cdot x_i^T \boldsymbol{A}^{-1} (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)} + y \cdot x_i) < 0 \right] \tag{66}$$

$$= \mathbb{I}\left[x_i^T \boldsymbol{A}^{-1} x_i + y_i \cdot x_i^T \boldsymbol{A}^{-1} (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)}) < 0 \right] \tag{67}$$

$$\leqslant \mathbb{I}\left[y_i \cdot x_i^T \boldsymbol{A}^{-1} (\boldsymbol{X}_{(i)}^T \boldsymbol{y}_{(i)}) < 0 \right] = \mathcal{E}(\widehat{f}_{(i)}(x_i), y_i)\,. \tag{68}$$

Using (68), we have

$$\mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathrm{LOO}(S_M)} := \frac{\sum_{(x_i, y_i) \in \widetilde{S}_M} \mathcal{E}(\widehat{f}_{(i)}(x_i), y_i)}{\left|\widetilde{\mathcal{S}}_M\right|} \tag{69}$$

Part 2 We now relate RHS in (69) with the population error on mislabeled distribution. To do this, we leverage Condition 1 and Lemma 12. In particular, we have

$$\mathbb{E}_{\mathcal{S} \cup \widetilde{\mathcal{S}}_M}\left[\left(\mathcal{E}_{\mathcal{D}'}(\widehat{f}) - \mathcal{E}_{\mathrm{LOO}(S_M)} \right)^2 \right] \leqslant \frac{1}{2m_1} + \frac{3\beta}{m+n}\,. \tag{70}$$

Using Chebyshev's inequality, with probability at least $1 - \delta$, we have

$$\mathcal{E}_{\mathrm{LOO}(S_M)} \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f}) + \sqrt{\frac{1}{\delta}\left(\frac{1}{2m_1} + \frac{3\beta}{m+n}\right)}\,. \tag{71}$$

Part 3 Combining (71) and (69), we have

$$\mathcal{E}_{\widetilde{\mathcal{S}}_M}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{D}'}(\widehat{f}) + \sqrt{\frac{1}{\delta}\left(\frac{1}{2m_1} + \frac{3\beta}{m+n}\right)}\,. \tag{72}$$

Compare (72) with (13) in the proof of Lemma 1. We obtain a similar relationship between $\mathcal{E}_{\widetilde{S}_M}$ and $\mathcal{E}_{\mathcal{D}'}$ but with a polynomial concentration instead of exponential concentration. In addition, since we just use concentration arguments to relate mislabeled error to the errors on the clean and unlabeled portions of the randomly labeled data, we can directly use the results in Lemma 2 and Lemma 3. Therefore, combining results in Lemma 2, Lemma 3, and (72) with union bound, we have with probability at least $1-\delta$

$$\mathcal{E}_{\mathcal{D}}(\widehat{f}) \leqslant \mathcal{E}_{\mathcal{S}}(\widehat{f}) + 1 - 2\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + \left(\sqrt{2}\mathcal{E}_{\widetilde{\mathcal{S}}}(\widehat{f}) + 1 + \frac{m}{2n}\right)\sqrt{\frac{\log(4/\delta)}{m}} + \sqrt{\frac{4}{\delta}\left(\frac{1}{m} + \frac{3\beta}{m+n}\right)}. \tag{73}$$

□

Discussion on Condition 1 The quantity in LHS of Condition 1 measures how much the function learned by the algorithm (in terms of error on unseen point) will change when one point in the training set is removed. Intuitively, Condition 1 states that empirical leave-one-out error and average population error of leave-one-out classifiers are close. We need hypothesis stability condition to control the variance of the empirical leave-one-out error to show concentration of average leave-one-error with the population error.

Additionally, we note that while the dominating term in the RHS of Theorem 3 matches with the dominating term in ERM bound in Theorem 4, there is a polynomial concentration term (dependence on $1/\delta$ instead of $\log(\sqrt{1/\delta})$) in Theorem 3. Since with hypothesis stability, we just bound the variance, the polynomial concentration is due to the use of Chebyshev's inequality instead of an exponential tail inequality (as in Lemma 1). Recent works have highlighted that a slightly stronger condition than hypothesis stability can be used to obtain an exponential concentration for leave-one-out error (Abou-Moustafa & Szepesvári, 2019), but we leave this for future work for now.

Extensions to kernel regression Since the result in Theorem 3 don't impose any regularity conditions on the underlying distribution over $\mathcal{X} \times \mathcal{Y}$, our guarantees straightforwardly extend to kernel regression by using the transformation $x \to \phi(x)$ for some feature transform function ϕ. Furthermore, recent literature has pointed out a concrete connection between neural networks and kernel regression with the so-called *Neural Tangent Kernel* (NTK) which holds in a certain regime where weights don't change much during training (Jacot et al., 2018; Du et al., 2019; 2018; Chizat et al., 2019). Using this concrete correspondence, our bounds on the clean population error (Theorem 3) extend to wide neural networks operating in the NTK regime.

Extensions to early stopped GD Often in practice, gradient descent is stopped early. We now provide theoretical evidence that our guarantees may continue to hold for an early stopped GD iterate. Concretely, we show that in expectation, the outputs of the GD iterates are close to that of a problem with data-independent regularization (as considered in Theorem 1). First, we define some notation. By $\mathcal{L}_S(w)$, we denote the objective in (2) with $\lambda = 0$. Consider the GD iterates defined in (58). Let $\widetilde{w}_\lambda = \arg\min_w \mathcal{L}_{\mathcal{S}}(w;\lambda)$. Define $f_t(x) := f(x; w_t)$ as the solution at the t^{th} iterate and $\widetilde{f}_\lambda(x) := f(x; \widetilde{w}_\lambda)$ as the regularized solution. Let κ be the condition number of the population covariance matrix and let $s_{\min}$ be the minimum positive singular value of the empirical covariance matrix.

Proposition 2 (informal)**.** *For $\lambda = \frac{1}{t\eta}$, we have*

$$\mathbb{E}_{x\sim\mathcal{D}_{\mathcal{X}}}\left[(f_t(x) - \widetilde{f}_\lambda(x))^2\right] \leqslant c(t,\eta)\cdot\mathbb{E}_{x\sim\mathcal{D}_{\mathcal{X}}}\left[f_t(x)^2\right],$$

where $c(t,\eta) \approx \kappa \cdot \min(0.25, \frac{1}{s_{min}^2 t^2 \eta^2})$. An equivalent guarantee holds for a point x sampled from the training data.

Remark Proposition 2 only bounds the expected squared difference between the t^{th} gradient descent iterate and a corresponding regularized solution. The expected squared difference and the expected difference of classification errors, that we wish to bound, are not related in general. They can however be related under standard low-noise (margin) assumptions. For instance, under the Tsybakov noise

condition (Tsybakov et al., 1997; Yao et al., 2007), we can lower bound the expression on the LHS of Proposition 2 with the difference of expected classification error.

The proposition above states that for large enough t, GD iterates stay close to a regularized solution with data-independent regularization constant. Together with our guarantees in Theorem 3 for regularization solution with $\lambda = \frac{1}{t\eta}$, Proposition 2 shows that our guarantees with RATT may hold on early stopped GD.

D.2 Formal statement and proof of of Proposition 2

Before formally presenting the result, we will introduce some notation. By $\mathcal{L}_S(w)$, we denote the objective in (57) with $\lambda = 0$. Assume Singular Value Decomposition (SVD) of $\boldsymbol{X}$ as $\sqrt{n}\boldsymbol{U}\boldsymbol{S}^{1/2}\boldsymbol{V}^T$. Hence $\boldsymbol{X}^T\boldsymbol{X} = \boldsymbol{V}\boldsymbol{S}\boldsymbol{V}^T$. Consider the GD iterates defined in (58). We now derive closed form expression for the t^{th} iterate of gradient descent:

$$w_t = w_{t-1} + \eta \cdot \boldsymbol{X}^T(\boldsymbol{y} - \boldsymbol{X}w_{t-1}) = (\boldsymbol{I} - \eta\boldsymbol{V}\boldsymbol{S}\boldsymbol{V}^T)w_{k-1} + \eta\boldsymbol{X}^T\boldsymbol{y}\,. \tag{74}$$

Rotating by $\boldsymbol{V}^T$, we get

$$\widetilde{w}_t = (\boldsymbol{I} - \eta\boldsymbol{S})\widetilde{w}_{k-1} + \eta\widetilde{\boldsymbol{y}}\,,, \tag{75}$$

where $\widetilde{w}_t = \boldsymbol{V}^T w_t$ and $\widetilde{\boldsymbol{y}} = \boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}$. Assuming the initial point $w_0 = 0$ and applying the recursion in (75), we get

$$\widetilde{w}_t = \boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^k)\widetilde{\boldsymbol{y}}\,, \tag{76}$$

Projecting solution back to the original space, we have

$$w_t = \boldsymbol{V}\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^k)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\,, \tag{77}$$

Define $f_t(x) := f(x; w_t)$ as the solution at the t^{th} iterate. Let $\widetilde{w}_\lambda = \arg\min_w \mathcal{L}_{\mathcal{S}}(w;\lambda) = (\boldsymbol{X}^T\boldsymbol{X} + \lambda\boldsymbol{I})^{-1}\boldsymbol{X}^T\boldsymbol{y} = \boldsymbol{V}(\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}$. and define $\widetilde{f}_\lambda(x) := f(x; \widetilde{w}_\lambda)$ as the regularized solution. Assume κ be the condition number of the population covariance matrix and let s_{min} be the minimum positive singular value of the empirical covariance matrix. Our proof idea is inspired from recent work on relating gradient flow solution and regularized solution for regression problems (Ali et al., 2018). We will use the following lemma in the proof:

Lemma 13. *For all $x \in [0,1]$ and for all $k \in \mathbb{N}$, we have (a) $\frac{kx}{1+kx} \leqslant 1 - (1-x)^k$ and (b) $1 - (1-x)^k \leqslant 2 \cdot \frac{kx}{kx+1}$.*

Proof. Using $(1-x)^k \leqslant \frac{1}{1+kx}$, we have part (a). For part (b), we numerically maximize $\frac{(1+kx)(1-(1-x)^k)}{kx}$ for all $k \geqslant 1$ and for all $x \in [0,1]$. □

Proposition 3 (Formal statement of Proposition 2)**.** *Let $\lambda = \frac{1}{t\eta}$. For a training point x, we have*

$$\mathbb{E}_{x\sim\mathcal{S}}\left[(f_t(x) - \widetilde{f}_\lambda(x))^2\right] \leqslant c(t,\eta) \cdot \mathbb{E}_{x\sim\mathcal{S}}\left[f_t(x)^2\right]\,,$$

where $c(t,\eta) := \min(0.25, \frac{1}{s_{min}^2 t^2\eta^2})$. Similarly for a test point, we have

$$\mathbb{E}_{x\sim\mathcal{D}_{\mathcal{X}}}\left[(f_t(x) - \widetilde{f}_\lambda(x))^2\right] \leqslant \kappa \cdot c(t,\eta) \cdot \mathbb{E}_{x\sim\mathcal{D}_{\mathcal{X}}}\left[f_t(x)^2\right]\,.$$

Proof. We want to analyze the expected squared difference output of regularized linear regression with regularization constant $\lambda = \frac{1}{\eta t}$ and the gradient descent solution at the t^{th} iterate. We separately expand the algebraic expression for squared difference at a training point and a test point. Then the main step is to show that $\left[\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^k) - (\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\right] \preceq c(\eta,t) \cdot \boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^k)$.

Part 1 First, we will analyze the squared difference of the output at a training point (for simplicity, we refer to $S \cup \widetilde{S}$ as S), i.e.,

$$\mathbb{E}_{x\sim\mathcal{S}}\left[\left(f_t(x)-\widetilde{f}_\lambda(x)\right)^2\right] = \|\boldsymbol{X}w_t - \boldsymbol{X}\widetilde{w}_\lambda\|_2^2 \tag{78}$$

$$= \left\|\boldsymbol{X}\boldsymbol{V}\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} - \boldsymbol{X}\boldsymbol{V}(\boldsymbol{S}+\lambda\boldsymbol{I})^{-1}\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\right\|_2^2 \tag{79}$$

$$= \left\|\boldsymbol{X}\boldsymbol{V}\left(\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t) - (\boldsymbol{S}+\lambda\boldsymbol{I})^{-1}\right)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\right\|_2 \tag{80}$$

$$= \boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left(\underbrace{\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t) - (\boldsymbol{S}+\lambda\boldsymbol{I})^{-1}}_{\text{I}}\right)^2\boldsymbol{S}\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} \tag{81}$$

We now separately consider term 1. Substituting $\lambda = \frac{1}{t\eta}$, we get

$$\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t) - (\boldsymbol{S}+\lambda\boldsymbol{I})^{-1} = \boldsymbol{S}^{-1}\left((\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t) - (\boldsymbol{I}+\boldsymbol{S}^{-1}\lambda)^{-1}\right) \tag{82}$$

$$= \underbrace{\boldsymbol{S}^{-1}\left((\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t)\right.}_{\boldsymbol{A}}\underbrace{\left.- (\boldsymbol{I}+(\boldsymbol{S}t\eta)^{-1})^{-1}\right)}_{\boldsymbol{A}} \tag{83}$$

We now separately bound the diagonal entries in matrix $\boldsymbol{A}$. With s_i, we denote i^{th} diagonal entry of $\boldsymbol{S}$. Note that since $\eta \leqslant 1/\|S\|_{\text{op}}$, for all i, $\eta s_i \leqslant 1$. Consider i^{th} diagonal term (which is non-zero) of the diagonal matrix $\boldsymbol{A}$, we have

$$\boldsymbol{A}_{ii} = \frac{1}{s_i}\left(1-(1-s_i\eta)^t - \frac{t\eta s_i}{1+t\eta s_i}\right) = \frac{1-(1-s_i\eta)^t}{s_i}\left(\underbrace{1-\frac{t\eta s_i}{(1+t\eta s_i)(1-(1-s_i\eta)^t)}}_{\text{II}}\right) \tag{84}$$

$$\leqslant \frac{1}{2}\left[\frac{1-(1-s_i\eta)^t}{s_i}\right]. \qquad \text{(Using Lemma 13 (b))}$$

Additionally, we can also show the following upper bound on term 2:

$$1-\frac{t\eta s_i}{(1+t\eta s_i)(1-(1-s_i\eta)^t)} = \frac{(1+t\eta s_i)(1-(1-s_i\eta)^t) - t\eta s_i}{(1+t\eta s_i)(1-(1-s_i\eta)^t)} \tag{85}$$

$$\leqslant \frac{1-(1-s_i\eta)^t - t\eta s_i(1-s_i\eta)^t}{(1+t\eta s_i)(1-(1-s_i\eta)^t)} \tag{86}$$

$$\leqslant \frac{1}{t\eta s_i}. \qquad \text{(Using Lemma 13 (a))}$$

Combining both the upper bounds on each diagonal entry $\boldsymbol{A}_{ii}$, we have

$$\boldsymbol{A} \preceq c_1(\eta,t)\cdot\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t), \tag{87}$$

where $c_1(\eta,t) = \min(0.5, \frac{1}{ts_i\eta})$. Plugging this into (81), we have

$$\mathbb{E}_{x\sim\mathcal{S}}\left[\left(f_t(x)-\widetilde{f}_\lambda(x)\right)^2\right] \leqslant c(\eta,t)\cdot\boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left(\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t)\right)^2\boldsymbol{S}\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} \tag{88}$$

$$= c(\eta,t)\cdot\boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left[\left(\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t)\right)\boldsymbol{S}\left(\boldsymbol{S}^{-1}(\boldsymbol{I}-(\boldsymbol{I}-\eta\boldsymbol{S})^t)\right)\right]$$
$$\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} \tag{89}$$

$$= c(\eta,t)\cdot\|\boldsymbol{X}w_t\|_2^2 \tag{90}$$

$$= c(\eta,t)\cdot\mathbb{E}_{x\sim\mathcal{S}}\left[\left(f_t(x)\right)^2\right], \tag{91}$$

where $c(\eta, t) = \min(0.25, \frac{1}{t^2 s_i^2 \eta^2})$.

Part 2 With $\mathbf{\Sigma}$, we denote the underlying true covariance matrix. We now consider the squared difference of output at an unseen point:

$$\mathbb{E}_{x\sim\mathcal{D}_\mathcal{X}}\left[\left(f_t(x) - \widetilde{f}_\lambda(x)\right)^2\right] = \mathbb{E}_{x\sim\mathcal{D}_\mathcal{X}}\left[\left\|x^T w_t - x^T \widetilde{w}_\lambda\right\|_2\right] \tag{92}$$

$$= \left\|x^T \boldsymbol{V}\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} - x^T\boldsymbol{V}(\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\right\|_2 \tag{93}$$

$$= \left\|x^T\boldsymbol{V}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t) - (\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\right)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\right\|_2 \tag{94}$$

$$= \boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t) - (\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\right)\boldsymbol{V}^T\mathbf{\Sigma}\boldsymbol{V} \tag{95}$$

$$\left((\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t) - (\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}\right)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} \tag{96}$$

$$\leqslant \sigma_{\text{max}} \cdot \boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left(\underbrace{\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t) - (\boldsymbol{S} + \lambda\boldsymbol{I})^{-1}}_{\text{I}}\right)^2\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\,, \tag{97}$$

where σ_{max} is the maximum eigenvalue of the underlying covariance matrix $\mathbf{\Sigma}$. Using the upper bound on term 1 in (87), we have

$$\mathbb{E}_{x\sim\mathcal{D}_\mathcal{X}}\left[\left(f_t(x) - \widetilde{f}_\lambda(x)\right)^2\right] \leqslant \sigma_{\text{max}} \cdot c(\eta, t) \cdot \boldsymbol{y}^T\boldsymbol{V}\boldsymbol{X}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t)\right)^2\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y} \tag{98}$$

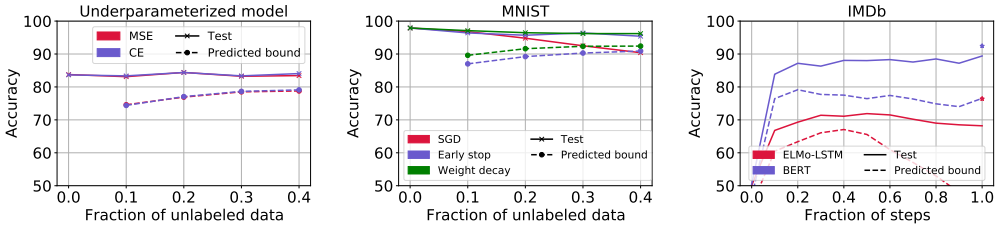
$$= \kappa \cdot c(\eta, t) \cdot \sigma_{\text{min}} \cdot \left\|\boldsymbol{V}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t)\right)\boldsymbol{V}^T\boldsymbol{X}^T\boldsymbol{y}\right\|_2^2 \tag{99}$$

$$\leqslant \kappa \cdot c(\eta, t) \cdot \left[\boldsymbol{V}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t)\right)\boldsymbol{V}^T\boldsymbol{X}^T\right]^T\mathbf{\Sigma} \tag{100}$$

$$\left[\boldsymbol{V}\left(\boldsymbol{S}^{-1}(\boldsymbol{I} - (\boldsymbol{I} - \eta\boldsymbol{S})^t)\right)\boldsymbol{V}^T\boldsymbol{X}^T\right]\boldsymbol{y} \tag{101}$$

$$= \kappa \cdot c(\eta, t) \cdot \mathbb{E}_{x\sim\mathcal{D}_\mathcal{X}}\left[\left\|x^T w_t\right\|_2\right]. \tag{102}$$

□



(a) (b) (c)

Figure 3: We plot the accuracy and corresponding bound (RHS in (1)) at $\delta = 0.1$. for binary classification tasks. Results aggregated over 3 seeds. (a) Accuracy vs fraction of unlabeled data (w.r.t clean data) in the toy setup with a linear model trained with GD. (b) Accuracy vs fraction of unlabeled data for a 2-layer wide network trained with SGD on binary MNIST. With SGD and no regularization (red curve in (b)), we interpolate the training data and hence the predicted lower bound is 0. However, with early stopping (or weight decay) we obtain tight guarantees. (c) Accuracy vs gradient iteration on IMDb dataset with unlabeled fraction fixed at 0.2. In plot (c), '*' denotes the best test accuracy with the same hyperparameters and training only on clean data.

E Detailed experiments

Having established our framework theoretically, we now demonstrate its utility experimentally. First, for linear models and wide networks in the NTK regime where our guarantee holds, we confirm that our bound is not only valid, but closely tracks the generalization error. Next, we show that in practical deep learning settings, optimizing cross-entropy loss by SGD, the expression for our (0-1) ERM bound nevertheless tracks test performance closely and in numerous experiments on diverse models and datasets is never violated empirically.

Note that the main lemma underlying our bound on (clean) population error states that when training on a mixture of clean and randomly labeled data, we obtain a classifier whose empirical error on the mislabeled training data is lower than its population error on the distribution of mislabeled data. While we prove this Lemma 1 for ERM on 0-1 loss, for linear models, and in the NTK regime, we must *assume it* to extend our bound to deep models. By way of justification, in the later stages of training, given the ability of neural networks to interpolate the data, this assumption seems uncontroversial. Moreover, concerning the early phases of training, recent research has shown that learning dynamics for complex deep networks resemble those for linear models (Nakkiran et al., 2019; Hu et al., 2020), much like the wide neural networks that we do analyze. Together, these arguments help to explain the practical applicability of our bound in deep learning.

Datasets To verify our results on linear models, we consider a toy dataset, where the class conditional distribution $p(x|y)$ for each label is Gaussian. For binary tasks, we use binarized CIFAR-10 (first 5 classes vs rest) (Krizhevsky & Hinton, 2009), binary MNIST (0-4 vs 5-9) (LeCun et al., 1998) and IMDb sentiment analysis dataset (Maas et al., 2011). For multiclass setup, we use MNIST and CIFAR-10.

Architectures To simulate the NTK regime, we experiment with 2-layered wide networks both (i) with the second layer fixed at random initialization; (ii) and updating both layers' weights. For vision datasets (e.g., MNIST and CIFAR10), we consider (fully connected) multilayer perceptrons (MLPs) with ReLU activations and ResNet18 (He et al., 2016). For the IMDb dataset, we train Long Short-Term Memory Networks (LSTMs; Hochreiter & Schmidhuber (1997)) with ELMo embeddings (Peters et al., 2018) and fine-tune an off-the-shelf uncased BERT model (Devlin et al., 2018; Wolf et al., 2020).

Methodology To bound the population error, we require access to both clean and unlabeled data. For toy datasets, we obtain unlabeled data by sampling from the underlying distribution over $\mathcal{X}$. For image and text datasets, we hold out a small fraction of the clean training data and discard their labels to simulate unlabeled data. We use the random labeling procedure described in preliminaries. After

Dataset	Model	Pred. Acc	Test Acc.	Best Acc.
MNIST	MLP	93.1	97.4	97.9
	ResNet	96.8	98.8	98.9
CIFAR10	MLP	48.4	54.2	60.0
	ResNet	76.4	88.9	92.3

Table 1: Results on multiclass classification tasks. With pred. acc. we refer to the dominating term in RHS of Theorem 2. At the given sample size and $\delta = 0.1$, the remaining term evaluates to 30.7, decreasing our predicted accuracy by the same. We note that test acc. denotes the corresponding accuracy on unseen clean data. Best acc. is the best achievable accuracy with just training on just the clean data (and same hyperparamters except the stopping point). Note that across all tasks our predicted bound is tight and the gap between the best accuracy and test accuracy is small.

augmenting clean training data with randomly labeled data, we train in the standard fashion. See App. E for experimental details.

Underparameterized linear models On toy Gaussian data, we train linear models on with GD to minimize cross-entropy loss and mean squared error. Varying the fraction of randomly labeled data we observe that the accuracy on clean unseen data is barely impacted (Fig. 3(left)). This highlights that in low dimensional models adding randomly labeled data with the clean dataset (in toy setup) has minimal effect on the performance on unseen clean data. Moreover, we find that RATT offers a tight lower bound on the unseen clean data accuracy. We observe the same behavior with Stochastic Gradient Descent (SGD) training (ref. App. E).

Wide Nets Next, we consider MNIST binary classification with a wide 2-layer fully-connected network. In experiments with SGD training on MSE loss without early stopping or weight decay regularization, we find that adding extra randomly label data hurts the unseen clean performance (Fig. 3(b)). Additionally, due to the perfect fit on the training data, our bound is rendered vacuous. However, with early stopping (or weight decay), we observe close to zero performance difference with additional randomly labeled data. Alongside, we obtain tight bounds on the accuracy on unseen clean data paying only a small price to negligible for incorporating randomly labeled data. Similar results hold for SGD and GD and when cross-entropy loss is substituted for MSE (ref. App. E).

Deep Nets We verify our findings on i) ResNet-18 and 5-layer MLPs trained with binary CIFAR (Fig. 1); and ii) ELMo-LSTM and BERT-Base models fine-tuned on the IMDb dataset (Fig. 3(c)). See App. E for additional results with deep models on binary MNIST. We fix the amount of unlabeled data at 20% of the clean dataset size and train all models with standard hyperparameters. Consistently, we find that our predicted bounds are never violated in practice. And as training proceeds, the fit on the mislabeled data increases with perfect overfitting in the interpolation regime rendering our bounds vacuous. However, with early stopping, our bound predicts test performance closely. For example, on IMDb dataset with BERT fine-tuning we predict 79.8 as the accuracy of the classifier, when the true performance is 88.04 (and the best achievable performance on unseen data is 92.45). Additionally, we observe that our method tracks the performance from the beginning of the training and not just towards the end.

Finally, we verify our bound multiclass bound on MNIST and CIFAR10 with deep MLPs and ResNets (see results in Table 1 and per-epoch curves in App. E). As before, we fix the amount of unlabeled data at 20% of the clean dataset to minimize cross-entropy loss via SGD. In all four settings, our bound predicts non-vacuous performance on unseen data. In App. E, we investigate our approach on CIFAR100 showing that even though our bound grows pessimistic with greater numbers of classes, the error on the mislabeled data nevertheless tracks population accuracy.

E.1 Additional details on Datasets

Toy Dataset Assume fixed constants μ and σ. For a given label y, we simulate features x in our toy classification setup as follows:

$$x := \texttt{concat}\left[x_1, x_2\right] \quad \text{where} \quad x_1 \sim \mathcal{N}(y \cdot \mu, \sigma^2 I_{d\times d}) \;\text{ and }\; x_1 \sim \mathcal{N}(0, \sigma^2 I_{d\times d})\,.$$

In experiements throughout the paper, we fix dimention $d = 100$, $\mu = 1.0$, and $\sigma = \sqrt{d}$. Intuitively, x_1 carries the information about the underlying label and x_2 is additional noise independent of the underlying label.

CV datasets We use MNIST (LeCun et al., 1998) and CIFAR10 Krizhevsky & Hinton (2009). We produce a binary variant from the multiclass classification problem by mapping classes $\{0, 1, 2, 3, 4\}$ to label 1 and $\{5, 6, 7, 8, 9\}$ to label -1. For CIFAR dataset, we also use the standard data augementation of random crop and horizontal flip. PyTorch code is as follows:

```
(transforms.RandomCrop(32, padding=4),
     transforms.RandomHorizontalFlip())
```

NLP dataset We use IMDb Sentiment analysis (Maas et al., 2011) corpus.

E.2 Additional Architectural Details

All experiments were run on NVIDIA GeForce RTX 2080 Ti GPUs. We used PyTorch (Paszke et al., 2019) and Keras with Tensorflow (Abadi et al., 2016) backend for experiments.

Linear model For the toy dataset, we simulate a linear model with scalar output and the same number of parameters as the number of dimensions.

Wide nets To simulate the NTK regime, we experiment with $2-$layered wide nets. The PyTorch code for 2-layer wide MLP is as follows:

```
nn.Sequential(
    nn.Flatten(),
    nn.Linear(input_dims, 200000, bias=True),
    nn.ReLU(),
    nn.Linear(200000, 1, bias=True)
    )
```

We experiment both (i) with the second layer fixed at random initialization; (ii) and updating both layers' weights.

Deep nets for CV tasks We consider a 4-layered MLP. The PyTorch code for 4-layer MLP is as follows:

```
nn.Sequential(nn.Flatten(),
    nn.Linear(input_dim, 5000, bias=True),
    nn.ReLU(),
    nn.Linear(5000, 5000, bias=True),
    nn.ReLU(),
    nn.Linear(5000, 5000, bias=True),
    nn.ReLU(),
    nn.Linear(1024, num_label, bias=True)
    )
```

For MNIST, we use 1000 nodes instead of 5000 nodes in the hidden layer. We also experiment with convolutional nets. In particular, we use ResNet18 (He et al., 2016). Implementation adapted from: `https://github.com/kuangliu/pytorch-cifar.git`.

Deep nets for NLP We use a simple LSTM model with embeddings intialized with ELMo embeddings (Peters et al., 2018). Code adapted from: `https://github.com/kamujun/elmo_experiments/blob/master/elmo_experiment/notebooks/elmo_text_classification_on_imdb.ipynb`

We also evaluate our bounds with a BERT model. In particular, we fine-tune an off-the-shelf uncased BERT model (Devlin et al., 2018). Code adapted from Hugging Face Transformers (Wolf et al., 2020): `https://huggingface.co/transformers/v3.1.0/custom_datasets.html`.

E.3 Additonal experiments

Results with SGD on underparameterized linear models

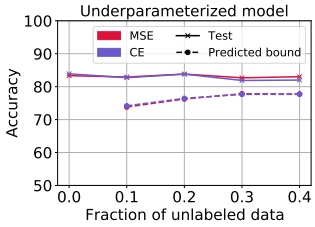
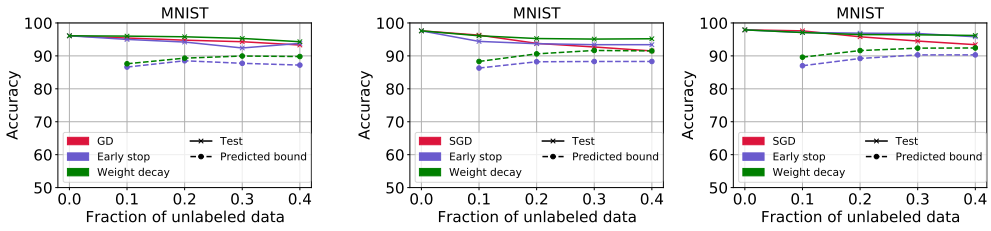


Figure 4: We plot the accuracy and corresponding bound (RHS in (1)) at $\delta = 0.1$ for toy binary classification task. Results aggregated over 3 seeds. Accuracy vs fraction of unlabeled data (w.r.t clean data) in the toy setup with a linear model trained with SGD. Results parallel to Fig. 3(a) with SGD.

Results with wide nets on binary MNIST



(a) GD with MSE loss (b) SGD with CE loss (c) SGD with MSE loss

Figure 5: We plot the accuracy and corresponding bound (RHS in (1)) at $\delta = 0.1$ for binary MNIST classification. Results aggregated over 3 seeds. Accuracy vs fraction of unlabeled data for a 2-layer wide network on binary MNIST with both the layers training in (a,b) and only first layer training in (c). Results parallel to Fig. 3(b) .

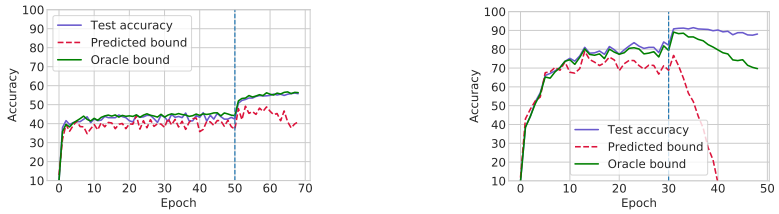
Results on CIFAR 10 and MNIST We plot epoch wise error curve for results in Table 1(Fig. 6 and Fig. 7). We observe the same trend as in Fig. 1. Additionally, we plot an *oracle bound* obtained by tracking the error on mislabeled data which nevertheless were predicted as true label. To obtain an exact emprical value of the oracle bound, we need underlying true labels for the randomly labeled data. While with just access to extra unlabeled data we cannot calculate oracle bound, we note that the oracle bound is very tight and never violated in practice underscoring an importamt aspect of generalization in multiclass problems. This highlight that even a stronger conjecture may hold in multiclass classification, i.e., error on mislabeled data (where nevertheless true label was predicted) lower bounds the population error on the distribution of mislabeled data and hence, the error on (a specific) mislabeled portion predicts the population accuracy on clean data. On the other hand, the dominating term of in Theorem 2 is loose when compared with the oracle bound. The main reason, we believe is the pessimistic upper bound in (41) in the proof of Lemma 8. We leave an investigation on this gap for future.

Results on CIFAR 100 On CIFAR100, our bound in Theorem 2 yields vacous bounds. However, the oracle bound as explained above yields tight guarantees in the initial phase of the learning (i.e., when learning rate is less than 0.1) (Fig. 8).

E.4 Hyperparameter Details

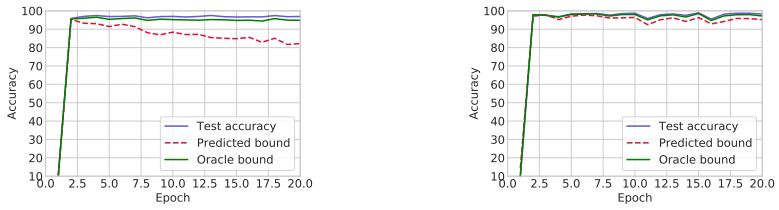
Fig. 1 We use clean training dataset of size $40,000$. We fix the amount of unlabeled data at 20% of the clean size, i.e. we include additional $8,000$ points with randomly assigned labels. We use test set of $10,000$ points. For both MLP and ResNet, we use SGD with an initial learning rate of 0.1 and momentum 0.9. We fix the weight decay parameter at 5×10^{-4}. After 100 epochs, we decay the learning rate to 0.01. We use SGD batch size of 100.

Fig. 3 (a) We obtain a toy dataset according to the process described in Sec. E.1. We fix $d = 100$ and create a dataset of $50,000$ points with balanced classes. Moreover, we sample additional covariates



(a) MLP (b) ResNet

Figure 6: Per epoch curves for CIFAR10 corresponding results in Table 1. As before, we just plot the dominating term in the RHS of Theorem 2 as predicted bound. Additionally, we also plot the predicted lower bound by the error on mislabeled data which nevertheless were predicted as true label. We refer to this as "Oracle bound". See text for more details.



(a) MLP (b) ResNet

Figure 7: Per epoch curves for MNIST corresponding results in Table 1. As before, we just plot the dominating term in the RHS of Theorem 2 as predicted bound. Additionally, we also plot the predicted lower bound by the error on mislabeled data which nevertheless were predicted as true label. We refer to this as "Oracle bound". See text for more details.

with the same procedure to create randomly labeled dataset. For both SGD and GD training, we use a fixed learning rate 0.1.

Fig. 3 (b) Similar to binary CIFAR, we use clean training dataset of size $40,000$ and fix the amount of unlabeled data at 20% of the clean dataset size. To train wide nets, we use a fixed learning of 0.001 with GD and SGD. We decide the weight decay parameter and the early stopping point that maximizes our generalization bound (i.e. without peeking at unseen data). We use SGD batch size of 100.

Fig. 3 (c) With IMDb dataset, we use a clean dataset of size $20,000$ and as before, fix the amount of unlabeled data at 20% of the clean data. To train ELMo model, we use Adam optimizer with a fixed learning rate 0.01 and weight decay 10^{-6} to minimize cross entropy loss. We train with batch size 32 for 3 epochs. To fine-tune BERT model, we use Adam optimizer with learning rate 5×10^{-5} to minimize cross entropy loss. We train with a batch size of 16 for 1 epoch.

Table 1 For multiclass datasets, we train both MLP and ResNet with the same hyperparameters as described before. We sample a clean training dataset of size $40,000$ and fix the amount of unlabeled data at 20% of the clean size. We use SGD with an initial learning rate of 0.1 and momentum 0.9. We fix the weight decay parameter at 5×10^{-4}. After 30 epochs for ResNet and after 50 epochs for MLP, we decay the learning rate to 0.01. We use SGD with batch size 100. For Fig. 8, we use the same hyperparameters as CIFAR10 training, except we now decay learning rate after 100 epochs.

In all experiments, to identify the best possible accuracy on just the clean data, we use the exact same set of hyperparamters except the stopping point. We choose a stopping point that maximizes test performance.

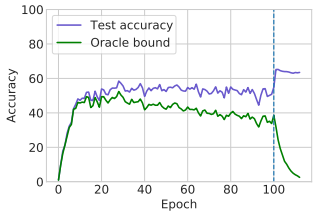


Figure 8: Predicted lower bound by the error on mislabeled data which nevertheless were predicted as true label with ResNet18 on CIFAR100. We refer to this as "Oracle bound". See text for more details. The bound predicted by RATT (RHS in Theorem 2) is vacuous.

E.5 SUMMARY OF EXPERIMENTS

Classification type	Model category	Model	Dataset
Binary	Low dimensional	Linear model	Toy Gaussain dataset
	Overparameterized linear nets	2-layer wide net	Binary MNIST
	Deep nets	MLP	Binary MNIST
			Binary CIFAR
		ResNet	Binary MNIST
			Binary CIFAR
		ELMo-LSTM model	IMDb Sentiment Analysis
		BERT pre-trained model	IMDb Sentiment Analysis
Multiclass	Deep nets	MLP	MNIST
			CIFAR10
		ResNet	MNIST
			CIFAR10
			CIFAR100

F PROOF OF LEMMA 12

Proof of Lemma 12. Recall, we have a training set $S \cup \widetilde{S}_C$. We defined leave-one-out error on mislabeled points as

$$\mathcal{E}_{\text{LOO}(\widetilde{S}_M)} = \frac{\sum_{(x_i,y_i)\in\widetilde{S}_M} \mathcal{E}(f_{(i)}(x_i), y_i)}{\left|\widetilde{S}_M\right|},$$

where $f_{(i)} := f(\mathcal{A}, (S \cup \widetilde{S})_{(i)})$. Define $S' := S \cup \widetilde{S}$. Assume (x, y) and (x', y') as i.i.d. samples from $\mathcal{D}'$. Using Lemma 25 in Bousquet & Elisseeff (2002), we have

$$\begin{aligned}\mathbb{E}\left[\left(\mathcal{E}_{\mathcal{D}'}(\widehat{f}) - \mathcal{E}_{\text{LOO}(\widetilde{S}_M)}\right)^2\right] \leqslant & \mathbb{E}_{S',(x,y),(x',y')}\left[\mathcal{E}(\widehat{f}(x), y)\mathcal{E}(\widehat{f}(x'), y')\right] - 2\mathbb{E}_{S',(x,y)}\left[\mathcal{E}(\widehat{f}(x), y)\mathcal{E}(f_{(i)}(x_i), y_i)\right] \\ & + \frac{m_1 - 1}{m_1}\mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i)\mathcal{E}(f_{(j)}(x_j), y_j)\right] + \frac{1}{m_1}\mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i)\right].\end{aligned} \tag{103}$$

We can rewrite the equation above as :

$$\begin{aligned}\mathbb{E}\left[\left(\mathcal{E}_{\mathcal{D}'}(\widehat{f}) - \mathcal{E}_{\text{LOO}(\widetilde{S}_M)}\right)^2\right] \leqslant & \underbrace{\mathbb{E}_{S',(x,y),(x',y')}\left[\mathcal{E}(\widehat{f}(x), y)\mathcal{E}(\widehat{f}(x'), y') - \mathcal{E}(\widehat{f}(x), y)\mathcal{E}(f_{(i)}(x_i), y_i)\right]}_{\text{I}} \\ & + \underbrace{\mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i)\mathcal{E}(f_{(j)}(x_j), y_j) - \mathcal{E}(\widehat{f}(x), y)\mathcal{E}(f_{(i)}(x_i), y_i)\right]}_{\text{II}} \\ & + \underbrace{\frac{1}{m_1}\mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i) - \mathcal{E}(f_{(i)}(x_i), y_i)\mathcal{E}(f_{(j)}(x_j), y_j)\right]}_{\text{III}}.\end{aligned} \tag{104}$$

We will now bound term III. Using Schwarz's inequality, we have

$$\mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i) - \mathcal{E}(f_{(i)}(x_i), y_i)\mathcal{E}(f_{(j)}(x_j), y_j)\right]^2 \leqslant \mathbb{E}_{S'}\left[\mathcal{E}(f_{(i)}(x_i), y_i)\right]^2 \mathbb{E}_{S'}\left[1 - \mathcal{E}(f_{(j)}(x_j), y_j)\right]^2 \tag{105}$$

$$\leqslant \frac{1}{4} \tag{106}$$

Note that since (x_i, y_i), (x_j, y_j), (x, y), and (x', y') are all from same distribution $\mathcal{D}'$, we directly incorporate the bounds on term I and II from proof of Lemma 9 in Bousquet & Elisseeff (2002). Combining that with (106) and our definition of hypothesis stability in Condition 1, we have the required claim.

□