On the Generalization Effects of Linear Transformations in Data Augmentation

Sen Wu *1  Hongyang R. Zhang *2  Gregory Valiant 1  Christopher Ré 1

Abstract
Data augmentation is a powerful technique to improve performance in applications such as image and text classification tasks. Yet, there is little rigorous understanding of why and how various augmentations work. In this work, we consider a family of linear transformations and study their effects on the ridge estimator in an over-parametrized linear regression setting. First, we show that transformations which preserve the labels of the data can improve estimation by enlarging the span of the training data. Second, we show that transformations which mix data can improve estimation by playing a regularization effect. Finally, we validate our theoretical insights on MNIST. Based on the insights, we propose an augmentation scheme that searches over the space of transformations by how uncertain the model is about the transformed data. We validate our proposed scheme on image and text datasets. For example, our method outperforms RandAugment by 1.24% on CIFAR-100 using Wide-ResNet-28-10. Furthermore, we achieve comparable accuracy to the SoTA Adversarial AutoAugment on CIFAR-10, CIFAR-100, SVHN, and ImageNet datasets.

1. Introduction
Data augmentation refers to the technique of enlarging the training dataset through pre-defined transformation functions. By searching over a (possibly large) space of transformations through reinforcement learning based techniques, augmentation schemes including AutoAugment (Cubuk et al., 2018) and TANDA (Ratner et al., 2017) have shown remarkable gains over various models on image classification tasks. Recent work has proposed random sampling (Cubuk et al., 2019) and Bayesian optimization (Hataya et al., 2019) to reduce the search cost, since RL-based techniques are computationally expensive. Despite the rapid progress of these transformation search methods, precisely understanding their benefits remains a mystery because of a lack of analytic tools. In this work, we study when and why applying a family of linear transformations helps from a theoretical perspective. Building on the theory, we develop methods to improve the efficiency of transformation search procedures.

A major challenge to understand the theory behind data augmentation is how to model the large variety of transformations used in practice in an analytically tractable framework. The folklore wisdom behind data augmentation is that adding more labeled data improves generalization, i.e. the performance of the trained model on test data (Shorten & Khoshgoftaar, 2019). Clearly, the generalization effect of an augmentation scheme depends on how it transforms the data. Previous work has analyzed the effect of Gaussian augmentation (Rajput et al., 2019) and feature averaging effect of adding transformed data (Duo et al., 2019; Chen et al., 2019). However, there is still a large gap between the transformations studied in these works and the ones commonly used in augmentation schemes.

In this work, we consider linear transformations which represent a large family of image transformations. We consider three categories: (i) Label-invariant (base) transformations such as rotation and horizontal flip; (ii) Label-mixing transformations including mixup (Zhang et al., 2017; Inoue, 2018), which produces new data by randomly mixing the features of two data points (e.g. a cat and a dog) – the labels are also mixed; (iii) Compositions of (label-invariant) transformations such as random cropping and rotating followed by horizontal flipping.

To gain insight into the effects of linear transformations, we consider a conceptually simple over-parametrized model proposed in Bartlett et al. (2019); Xie et al. (2020); Hastie et al. (2019) that captures the need to add more data as in image settings. Suppose we are given \( n \) training data points \( x_1, \ldots, x_n \in \mathbb{R}^p \) as \( X \in \mathbb{R}^{n \times p} \) with labels \( Y \in \mathbb{R}^n \). In this setting, the labels obey the linear model under ground truth parameters \( \beta \in \mathbb{R}^p \), i.e. \( Y = X \beta + \varepsilon \), where \( \varepsilon \in \mathbb{R}^n \) denotes i.i.d. random noise with mean zero and variance \( \sigma^2 \).

Importantly, we assume that \( p > n \), hence the span of the training data points does not include the entire space...
Building on our theory, we propose an algorithmic result. We provide the validation on MNIST in Section 4. We can show their effect for adding new information as a corollary of the base case (see Corollary 3.4 for details and proof). Finally, for compositions of label-invariant transformations, we can show their effect for adding new information as a corollary of the base case (see Corollary 3.4 for details and proof).

**Algorithmic results.** Building on our theory, we propose an uncertainty-based random sampling scheme which, among the transformed data points, picks those with the highest loss, i.e., "providing the most information". We find that there is a large variance among the performance of different transformations and their compositions. Unlike RandAugment (Cubuk et al., 2019), which averages the effect of all transformations, the idea behind our sampling scheme is to better select the transformations with strong performance.

We show that our proposed scheme applies to a wide range of datasets and models. First, our sampling scheme achieves higher accuracy by finding more useful transformations compared to RandAugment on three different CNN architectures. For example, our method outperforms RandAugment by 0.59% on CIFAR-10 and 1.24% on CIFAR-100 using Wide-ResNet-28-10, and 1.54% on ImageNet using ResNet-50. Figure 1 shows the key insight behind our proposed method. We compare the frequencies of transformations (cf. Section 5 for their descriptions) sampled by our method. As the training procedure progresses, our method gradually learns transformations providing new information (e.g. Rotate followed by ShearY) and reduces their frequencies. On the other hand, the frequencies of transformations such as Mixup followed by Equalize increase because they produce samples with large errors that the model cannot learn.

Second, we achieve similar test accuracy on CIFAR-10 and CIFAR-100 compared to the state-of-the-art Adversarial AutoAugment (Zhang et al., 2020). By contrast, our scheme is conceptually simpler and computationally more efficient; since our scheme does not require training an additional adversarial network, the training cost reduces by at least 5x. By further enlarging number of augmented samples by 4 times, we achieve test accuracy by at least 5x. By further enlarging number of augmented samples by 4 times, we achieve test accuracy by at least 5x.

**Notations.** We use the big-O notation \( f(n) \leq O(g(n)) \) to indicate that \( f(n) \leq C \cdot g(n) \) for a fixed constant \( C \) and large enough \( n \). We use \( f(n) \preceq g(n) \) to denote that \( f(n) \leq O(g(n)) \). For a matrix \( X \in \mathbb{R}^{d_1 \times d_2} \), let \( X^\dagger \) denote the Moore-Penrose psuedoinverse of \( X \).

<table>
<thead>
<tr>
<th>Transformations</th>
<th>Example</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label-invariant</td>
<td>Rotate ((F))</td>
<td>(((\beta^T P_X^T F x)^2/\beta^T F x)^2)</td>
</tr>
<tr>
<td>Label-mixing</td>
<td>Mixup</td>
<td>(</td>
</tr>
<tr>
<td>Composition</td>
<td>Rotate and flip ((F_1 F_2))</td>
<td>(((\beta^T P_X^T F_1 F_2 x)^2/\beta^T P_X^T F_1 F_2 x)^2)</td>
</tr>
</tbody>
</table>

Table 1. Illustrative examples of our theoretical results. For label-invariant transformations and their compositions, they can reduce the estimation error at a rate proportional to the added information. Label-mixing reduces estimation error through a regularization effect.

Figure 1. Our method learns and reduces the frequencies of the better performing transformations during training. Base model: PyramidNet+ShakeDrop (Han et al., 2017; Yamada et al., 2018). Dataset: CIFAR-10. See Section 5.3 for the details.
2. Preliminaries

Recall that \( X = [x_1^T, \ldots, x_n^T] \in \mathbb{R}^{n \times p} \) denotes the training data, where \( x_i \in \mathbb{R}^p \) for \( 1 \leq i \leq n \). Let \( \text{Id}_p \in \mathbb{R}^{p \times p} \) denote the identity matrix. Let \( P_X \) denote the projection matrix onto the row space of \( X \). Let \( P_X^\perp = \text{Id}_p - P_X \) denote the projection operator which is orthogonal to \( P_X \). The ridge estimator with parameter \( \lambda < 1 \) is given by

\[
\hat{\beta}(X, Y) = (X^T X + n \lambda \text{Id})^{-1} X^T Y,
\]

which arises from solving the mean squared loss

\[
\frac{1}{2n} \min_{w \in \mathbb{R}^p} ||Xw - Y||_F^2 + \frac{\lambda}{2} ||w||_2^2.
\]

We use \( \hat{\beta}^F \) to denote the ridge estimator when we augment \((X, Y)\) using a transformation function \( F \). The estimation error of \( \hat{\beta} \) is given by \( e(\hat{\beta}) := \mathbb{E}_\varepsilon ||\hat{\beta} - \beta||^2_2 \). Next we define the label-invariance property for regression settings.

**Definition 2.1** (Label-invariance). For a matrix \( F \in \mathbb{R}^{p \times p} \), we say that \( F \) is label-invariant over \( X \subseteq \mathbb{R}^p \) for \( \beta \in \mathbb{R}^p \) if

\[
x^T \beta = (Fx)^T \beta, \text{ for any } x \in X.
\]

As an example, consider a 3-D setting where \( X = \{ (a, b, 0) : \forall a, b \in \mathbb{R} \} \). Let \( \beta = (1, -1/2, 1/2)^T \) and

\[
F = \begin{pmatrix}
1 & 0 & 0 \\
0 & \cos \frac{\pi}{2} & \sin \frac{\pi}{2} \\
0 & -\sin \frac{\pi}{2} & \cos \frac{\pi}{2}
\end{pmatrix}.
\]

Then \((\text{Id} - F^T)\beta = (0, 0, 1)\) is orthogonal to \( X \). Hence \( F \) is a label-preserving rotation with degree \( \frac{\pi}{2} \) over \( X \) for \( \beta \).

In addition to rotations and mixup which we have described, linear transformations are capable of modeling many image transformations. We list several examples below.

**Horizontal flip.** The horizontal flip of a vector along its center can be written as an orthonormal transformation where

\[
F = \begin{pmatrix}
0 & \ldots & 0 & 1 \\
0 & \ldots & 1 & 0 \\
1 & \ldots & 0 & 0
\end{pmatrix}.
\]

**Additive composition.** For two transformations \( F_1 \) and \( F_2 \), their additive composition gives \( x^{\text{aug}} = F_1 x + F_2 x \). For example, changing the color of an image and adding Gaussian noise is an additive composition with \( F_1 x \) being a color transformation and \( F_2 x \) being a Gaussian perturbation.

**Multiplicative composition.** In this case, \( x^{\text{aug}} = F_1 F_2 x \). For example, a rotation followed by a cutout of an image is a multiplicative composition with \( F_2 \) being a rotation matrix and \( F_1 \) being a matrix which zeros out certain regions of \( x \).

### 3. Analyzing the Effects of Transformation Functions in an Over-parametrized Model

How should we think about the effects of applying a transformation? Suppose we have an estimator \( \hat{\beta} \) for a linear model \( \beta \in \mathbb{R}^p \). The bias-variance decomposition of \( \hat{\beta} \) is

\[
e(\hat{\beta}) = \mathbb{E}_\varepsilon \|\hat{\beta} - \beta\|^2 + \mathbb{E}_\varepsilon \|\hat{\beta} - \mathbb{E}_\varepsilon [\hat{\beta}]\|^2.
\]

In the context of data augmentation, we show the following two effects from applying a transformation.

**Adding new information.** The bias part measures the error of \( \hat{\beta} \) after taking the expectation of \( \varepsilon \) in \( \beta \). Intuitively, the bias part measures the intrinsic error of the model after taking into account the randomness which is present in \( \hat{\beta} \). A transformation may improve the bias part if \( x^{\text{aug}} \) is outside \( P_X \). We formalize the intuition in Section 3.1.

**Regularization.** Without adding new information, a transformation may still reduce \( e(\hat{\beta}) \) by playing a regularization effect. For example with mixup, \( x^{\text{aug}} \) is in \( P_X \). Hence adding \( x^{\text{aug}} \) does not add new information to the training data. However, the mixup sample reweights the training data and the \( \ell_2 \) regularization term in the ridge estimator. We quantify the effect in Section 3.2.

#### 3.1. Label-Invariant Transformations

We quantify the effect of label-invariant transformations which add new information to the training data.

**Example.** Given a training data point \((x, y)\), let \((x^{\text{aug}}, y^{\text{aug}})\) denote the augmented data where \( y^{\text{aug}} = y \). Intuitively, based on our training data \((X, Y)\), we can infer the label of any data point within \( P_X \) (e.g. when \( \sigma \) is sufficiently small). If \( x^{\text{aug}} \) satisfies \( P_X x^{\text{aug}} = 0 \), then adding \((x^{\text{aug}}, y^{\text{aug}})\) does not provide new information. On the other hand if \( P_X x^{\text{aug}} \neq 0 \), then adding \( x^{\text{aug}} \) expands the subspace over which we can obtain accurate estimation. Moreover, the added direction corresponds to \( P_X x^{\text{aug}} \). Meanwhile, since \( y^{\text{aug}} = y \), it contains a noise part which is correlated with \( \varepsilon \). Hence the variance of \( \hat{\beta} \) may increase.

To derive the result, we require a technical twist: instead of adding the transformed data \( Fx \) directly, we are going to add its projection onto \( P_X^\perp \). This is without loss of generality since we can easily infer the label of \( P_X^\perp Fx \). Let \( \hat{\beta}^F \) denote the ridge estimator after adding the augmented data to the \((X, Y)\). Our result is stated as follows.

**Theorem 3.1.** Suppose we are given a set of \( n \) covariates \( X \in \mathbb{R}^{n \times p} \) with labels \( Y = X \beta + \varepsilon \), where \( \beta \in \mathbb{R}^p \) and \( \varepsilon \in \mathbb{R}^n \) has mean 0 and variance \( \sigma^2 \). Let \( F \in \mathbb{R}^{p \times p} \) be a label-invariant transformation over \( X \) for \( \beta \). Let \((x, y)\) be a data point from \((X, Y)\).
Algorithm 1 Uncertainty-based sampling of transformations

1: Input. a batch of $B$ data point $(x_1, y_1), (x_2, y_2), \ldots, (x_B, y_B)$

Require. $K$ transformations $F_1, F_2, \ldots, F_K$, the current model $\hat{\beta}$ and the associated loss $l_{\hat{\beta}}$. Default transformations $G_1, \ldots, G_H$.

Param. $L$: number of composition steps; $C$: number of augmented data per input data; $S$: number of selected data points used for training.

Return: a list of $B \cdot S$ transformed data $T$.

2: for $i = 1, \ldots, B$ do
3:  for $k = 1, \ldots, C$ do
4:  Let $F_j^1, \ldots, F_j^K$ be $L$ transformations sampled uniformly at random without replacement from $F_1, \ldots, F_K$.
5:  Compute $x_k^{aug}$ and $y_k^{aug}$ by applying $F_j^1, \ldots, F_j^K$ and the default ones $G_1, \ldots, G_H$ sequentially on $(x_i, y_i)$.
6:  Infer the loss of $(x_k^{aug}, y_k^{aug})$ as $l^k = l_{\hat{\beta}}(x_k^{aug}, y_k^{aug})$.
7:  end for
8:  Choose the $S$ data points from $\{x_k^{aug}, y_k^{aug}\}_{k=1}^C$ that have the highest losses $l^k$ and add them to $T$.
9: end for

Let $z = P_X^† F x$ and $y^{aug} = y - \text{Diag} \left( (X^\top)^† F x \right) Y$. Suppose that we augment $(X, Y)$ with $(z, y^{aug})$. Then, we have that

$$
e(\hat{\beta}) - e(\beta^F) \geq \frac{2\lambda(n+1) - (1 - 2\lambda) \Vert z \Vert^2}{\lambda^2(n+1)^2} \cdot \hat{\beta} \cdot \beta^2 - \frac{(2 + 2 \Vert P_X F x \Vert^2_2 + \sigma^2 \Vert z \Vert^2}{\lambda^2(n+1)^2} \cdot \beta^2 \cdot \beta^2. \quad (2)$$

Moreover, when $\Vert z \Vert^2 = o(n)$ and $\frac{(z, \beta^2)}{\Vert z \Vert^2} \geq \log n(1 + \frac{\Vert P_X F x \Vert^2_2}{\mu_{min}(X)^2}) \sigma^2 \frac{\Vert z \Vert^2}{\lambda n}$ (including $\sigma = 0$), we have

$$0 \leq e(\hat{\beta}) - e(\beta^F) - (2 + o(1)) \frac{(z, \beta^2)}{\lambda n} \leq \frac{\text{poly}(\gamma/\lambda)}{n^2}. \quad (3)$$

In the above, $\mu_{min}(X)$ denotes the smallest singular value of $X$. For a vector $v$, $\text{Diag} [v] \in \mathbb{R}^{d \times d}$ denotes a diagonal matrix with the $i$-th diagonal entry being the $i$-th entry of $v$. $\text{poly}(\gamma/\lambda)$ denotes a polynomial of $\gamma/\lambda$.

Theorem 3.1 shows that the reduction of estimation error scales with $(z, \beta)^2$, the correlation between the new signal and the true model. Intuitively, as long as $n$ is large enough, then equation (3) will hold. The proof is by carefully comparing the bias and variance of $\hat{\beta}$ and $\hat{\beta}^{aug}$ after adding the augmented data point. On the other hand, we remark that adding $F x$ directly into $X$ does not always reduce $e(\hat{\beta})$, even when $(z, \beta)^2 = \Theta(1)$ (cf. (Xie et al., 2020)).

Another remark is that for augmenting a sequence of data points, one can repeatedly apply Theorem 3.1 to get the result. We leave the details to Appendix A.1.

Connection to augmentation sampling schemes. We derive a corollary for the idea of random sampling used in RandAugment. Let $\{F_j\}_{j=1}^K$ be a set of $K$ label-invariant transformations. We consider the effect of randomly sampling a transformation from $\{F_j\}_{j=1}^K$.

Corollary 3.2. In the setting of Theorem 3.1, let $\{F_j\}_{j=1}^K$ be $K$ label-invariant transformations. For a data point $(x, y)$ from $(X, Y)$ and $i = 1, \ldots, K$, let $z_i = P_X^† F_i x$ and $y_i^{aug} = y - \text{Diag} \left( (X^\top)^† F_i x \right) Y$.

Suppose that $(z_i, y_i^{aug})$ is chosen uniformly at random from $\{z_i, y_i^{aug}\}_{i=1}^K$. Then we have that

$$\mathbb{E}_{z, y^{aug}} \left[ e(\hat{\beta}) - e(\beta^{aug}(F_1, \ldots, F_K)) \right]$$

$$\leq \frac{2 + o(1)}{K} \left( \sum_{i=1}^K (z, \beta)^2 \right) + \frac{\text{poly}(\gamma/\lambda)}{n^2}. \quad (3)$$

The proof follows directly from Theorem 3.1. Corollary 3.2 implies that the effect of random sampling is simply an average over all the transformations. However, if there is a large variance among the effects of the $K$ transformations, random sampling could be sub-optimal.

**Our proposed scheme: uncertainty-based sampling.**

Our idea is to use the sampled transformations more efficiently via an *uncertainty-based* sampling scheme. For each data point, we randomly sample $C$ (compositions of) transformations. We pick the ones with the highest losses after applying the transformation. This is consistent with the intuition of Theorem 3.1. The larger $(z, \beta)^2$, the higher the loss of $(x^{aug}, y^{aug})$ would be under $\hat{\beta}$.

Algorithm 1 describes our procedure in detail. In Line 4-6, we compute the losses of $C$ augmented data points. In Line 8, we select the $S$ data points with the highest losses for training. For each batch, the algorithm returns $SB$ augmented samples.

3.2. Label-Mixing Transformations: Mixup

We show that mixup plays a regularization effect through reweighting the training data and the $\ell_2$ regularization term.

Specifically, we analyze the following procedure. Let $\alpha \in [0, 1]$ be sampled from a Beta distribution with fixed parameters (Zhang et al., 2017). Let $(x_i, y_i)$ and $(x_j, y_j)$ be two data points selected uniformly at random from the train-
We remark that the assumption that

\[ y_{\text{mixup}} = \alpha y_1 + (1 - \alpha) y_2 \]

We illustrate that adding the mixup sample is akin to shrinking the training data relative to the regularization term. Assuming that \( \sum_{i=1}^{n} x_i = 0 \), we have

\[
\mathbb{E}_{x_{\text{mixup}}} \left[ x_{\text{mixup}}^\top x_{\text{mixup}} \right] = \frac{1 - 2\alpha^2}{n} \cdot X^\top X \\
\Rightarrow \mathbb{E}_{x_{\text{mixup}}} \left[ X^\top X + x_{\text{mixup}}^\top x_{\text{mixup}} + (n + 1)\lambda \text{Id} \right] \\
= (1 + \frac{1 - 2\alpha^2}{n}) X^\top X + (n + 1)\lambda \text{Id},
\]

Hence the mixup sample shrinks the \( X^\top X \) term relative to the \( \ell_2 \) regularization term in \( \beta_{\text{mixup}} \). Below we describe our result formally.

**Theorem 3.3.** Let \( \gamma > 1 \) be a fixed constant which does not grow with \( n \). Let \( \{x_k\}_{k=1}^{n} \) be \( n \) training samples which satisfy that \( \sum_{k=1}^{n} x_k = 0 \) and \( \|x_k\| \leq \gamma \), for all \( 1 \leq k \leq n \), Assume that \( n \) is large enough (e.g. \( n \geq \frac{(\gamma + \lambda)^3}{\lambda^2} \max(\|\beta\|^4,\sigma^2\gamma) \)). In expectation over the randomness of \( \alpha, x_1, x_2 \), we have that

\[
\mathbb{E}_{\alpha, x_1, x_2} \left[ e(\beta) - e(\beta_{\text{mixup}}) \right] \geq \frac{\lambda^2 \|X\|_F^2}{\gamma^3} \frac{n^2}{\lambda n^2}.
\]

We remark that the assumption that \( \sum_{i=1}^{n} x_i = 0 \) is indeed satisfied in image classification settings. This is because a normalization step, which normalizes the mean of every RGB channel to be zero, is applied on all the images. The intuition behind the proof of Theorem 3.3 is that the mixup sample shrinks the training data, which reduces the bias of the estimator. The proof can be found in Appendix A.2.

### 3.3. Compositions of Label-Invariant Transformations

Our theory can also be applied to quantify the amount of new information added by compositions of transformations. We first describe an example to show that taking compositions expands the search space of transformation functions.

**Example.** Consider two transformations \( F_1 \) and \( F_2 \), e.g. a rotation and a horizontal flip. Suppose we are interested in finding a transformed sample \( (x_{\text{aug}}, y_{\text{aug}}) \) such that adding the sample reduces the estimation error of \( \beta_{\text{aug}} \) the most. With additive compositions, the search space for \( x_{\text{aug}} \) becomes

\[
\{ Fx : x \in \mathcal{X}, F \in \{ F_1, F_2, F_1 + F_2 \} \},
\]

which is strictly a superset compared to using \( F_1 \) and \( F_2 \).

Based on Theorem 3.1, we can derive a simple corollary which quantifies the incremental benefit of additively composing a new transformation.

**Corollary 3.4.** In the setting of Theorem 3.1, let \( F_1, F_2 \) be two label-invariant transformations. For a data point \( (x, y) \) from \( (X, Y) \) and \( i \in \{1, 2\} \), let \( z_i = P_X F_i x \) and \( y_{\text{aug}} = y - \text{Diag} \left( [X^\top]^\dagger F_i x \right) \). The benefit of composing \( F_2 \) with \( F_1 \) is given as follows

\[
e(\beta_{F_1}) - e(\beta_{F_1+F_2}) = (2 + o(1)) \left( \frac{z_1, \beta^2}{\lambda n} + \frac{\text{poly}(\gamma/\lambda)}{n^2} \right).
\]

Corollary 3.4 implies that the effect of composing \( F_2 \) with \( F_1 \) may either be better or worse than applying \( F_1 \). This is consistent with our experimental observation (described in Section 4). We defer the proof of Corollary 3.4 to Appendix A.3. We remark that the example and the corollary also apply to multiplicative compositions.

### 4. Measuring the Effects of Transformation Functions

We validate the theoretical insights from Section 3 on MNIST (LeCun et al., 1998). To extend our results from the regression setting to the classification setting, we propose two metrics that correspond to the bias and the variance of a linear model. Our idea is to decompose the average prediction accuracy (over all test samples) into two parts similar to equation (1), including an intrinsic error score which is deterministic and an instability score which varies because of randomness.

We show three claims: i) Label-invariant transformations such as rotations can add new information by reducing the intrinsic error score. ii) As we increase the fraction of same-class mixup digits, the instability score decreases. iii) Composing multiple transformations can either increase the accuracy (and intrinsic error score) or decrease it. Further, we show how to select a core set of transformations.

**Metrics.** We train \( k \) independent samples of multi-layer perceptron with hidden layer dimension 100. Let \( \hat{\beta}_i \) denote the predictor of the \( i \)-th sample, for \( 1 \leq i \leq k \). For each data point \( x \), let \( M(x) \) denote the majority label in \( \{\hat{\beta}_1, \ldots, \hat{\beta}_k\} \) (we break ties randomly). Clearly, the majority label is the best estimator one could get, given the \( k \) independent predictors, without extra information. Then, we define the **intrinsic error score** as

\[
\frac{1}{n} \cdot \left( \sum_{(x, y) \in (X, Y)} \mathbb{1}\{M(x) \neq y\} \right).
\]

We define the **instability score** as

\[
\frac{1}{n} \cdot \left( \sum_{(x, y) \in (X, Y)} \left( \frac{1}{k} \sum_{i=1}^{k} \mathbb{1}\{\hat{\beta}_i(x) \neq M(x)\} \right) \right).
\]
Table 2. Measuring the intrinsic error and instability scores of individual transformations on MNIST. The three transformations all reduce the intrinsic error score compared to the baseline.

<table>
<thead>
<tr>
<th>Transformation</th>
<th>Avg. Acc.</th>
<th>Error</th>
<th>Instab. Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>98.08%</td>
<td>1.52%</td>
<td>0.95%</td>
</tr>
<tr>
<td>Cutout</td>
<td>98.31%</td>
<td>1.43%</td>
<td>0.86%</td>
</tr>
<tr>
<td>RandCrop</td>
<td>98.61%</td>
<td>1.01%</td>
<td>0.88%</td>
</tr>
<tr>
<td>Rotation</td>
<td>98.65%</td>
<td>1.08%</td>
<td>0.77%</td>
</tr>
</tbody>
</table>

Compared to equation (1), the first score corresponds to the bias of $\hat{\beta}$, which can change if we add new information to the training data. The second score corresponds to the variance of $\hat{\beta}$, which measures the stability of the predicted outcomes in the classification setting. For the experiments we sample 9 random seeds, i.e. set $k = 9$.

**Label-invariant transformations.** Recall that Section 3.1 shows that label-invariant transformations can reduce the bias of a linear model by adding new information to the training data. Correspondingly, our hypothesis is that the intrinsic error score should decrease after augmenting the training dataset with suitable transformations.

Table 2 shows the result for applying rotation, random cropping and the cutout (i.e. cutting out a piece of the image) respectively. The baseline corresponds to using no transformations. We observe that the three transformations all reduce the model error score and the instability score, which confirms our hypothesis. There are also two second-order effects: i) A higher instability score hurts the average prediction accuracy of random cropping compared to rotation. ii) A higher intrinsic error score hurts the average prediction accuracy of cutout compared to random cropping.

To further validate that rotated data “adds new information”, we show that the intrinsic error score decreases by correcting data points that are “mostly incorrectly” predicted by the baseline model. Among the data points that are predicted correctly after applying the rotation but are wrong on the baseline model, the average accuracy of these data points on the baseline model is 25%. In other words, for 75% of the time, the baseline model makes the wrong prediction for these data. We leave the details to Appendix B.

**Label-mixing transformations.** Section 3.2 shows that in our regression setting, adding a mixup sample has a regularization effect. What does it imply for classification problems? We note that our regression setting comprises a single parameter class $\beta$. For MNIST, there are 10 different classes of digits. Therefore, a plausible hypothesis following our result is that mixing same-class digits has a regularization effect.

We conduct the following experiment to verify the hypothesis. We vary the fraction of mixup data from mixing same-class vs. different-class digits. We expect that as we increase the same class mixing fraction, the instability score decreases. The results of figure 2 confirm our hypothesis. We also observe that mixing different class images behaves differently compared to mixing same class images. The details are left to Appendix D.

**Compositions of transformations.** Recall that Section 3.3 shows the effect of composing two transformations may be positive or negative. We describe examples to confirm the claim. By composing rotation with random cropping, we observe an accuracy of 98.72% with intrinsic error score 0.86%, which are both lower than rotation and random cropping individually. A negative example is that composing translating the X and Y coordinate (acc. 98.0%) is worse than translating X (acc. 98.38%) or Y (acc. 98.19%) individually. Same for the other two scores.

**Identifying core transformations.** As an in-depth study, we select five transformation including rotation, random cropping, cutout, translation of the x-axis and the y-axis. These transformations can all change the geometric position of the digits in the image. Our goal is to identify a subset of core transformations from the five transformations. For example, since the rotation transformation implicitly changes the x and the y axis of the image, a natural question is whether composing translations with rotation helps or not.

To visualize the results, we construct a directed graph with the five transformations. We compose two transformations to measure their model error scores. An edge from transformation A to transformation B means that applying B after A reduces the model error score by over 10%. Figure 3 shows the results. We observe that rotation, random cropping and cutout can all help some other transformations, whereas the translations do not provide an additional benefit for the rest.
5. Experiments

We test our uncertainty-based transformation sampling scheme on both image and text classification tasks. First, our sampling scheme achieves more accurate results by finding more useful transformations compared to RandAugment. Second, we achieve comparable test accuracy to the SoTA Adversarial AutoAugment on CIFAR-10, CIFAR-100, and ImageNet with less training cost because our method is conceptually simpler. Finally, we evaluate our scheme in text augmentations to help train a sentiment analysis model.

5.1. Experimental Setup

Datasets and models. We consider the following datasets and models in our experiments.

**CIFAR-10 and CIFAR-100**: The two datasets are colored images with 10 and 100 classes, respectively. We evaluate our proposed method for classifying images using the following models: Wide-ResNet-28-10 (Zagoruyko & Komodakis, 2016), Shake-Shake (26×2×96d) (Gastaldi, 2017), and PyramidNet+ShakeDrop (Han et al., 2017; Yamada et al., 2018).

**Street view house numbers (SVHN)**: This dataset contains color house-number images with 73,257 core images for training and 26,032 digits for testing. We use Wide-ResNet-28-10 model for classifying these images.

**ImageNet Large-Scale Visual Recognition Challenge (ImageNet)**: This dataset includes images of 1000 classes, and has a training set with roughly 1.3M images, and a validation set with 50,000 images. We select ResNet-50 (He et al., 2016) to evaluate our method.

Comparison methods. For image classification tasks, we compare Algorithm 1 with AutoAugment (AA) (Cubuk et al., 2018), Fast AutoAugment (Fast AA) (Lim et al., 2019), Population Based Augmentation (PBA) (Ho et al., 2019), RandAugment (RA) (Cubuk et al., 2019), and Adversarial AutoAugment (Adv. AA) (Zhang et al., 2020). We also include the baseline model with the following default setting. For CIFAR-10 and CIFAR-100, we flip each image horizontally with probability 0.5 and then randomly crop a $32 \times 32$ sub-image from the padded image. For SVHN, we apply the cutout to every image. For ImageNet, we randomly resize and crop a $224 \times 224$ sub-image from the original image and then flip the image horizontally with probability 0.5.

Training procedures. Recall that Algorithm 1 contains three parameters, how many composition steps ($L$) we take, how many augmented data points ($C$) we generate and how many ($S$) we select for training. We set $L = 2$, $C = 4$ and $S = 1$ for our experiments on CIFAR datasets and SVHN. We set $L = 2$, $C = 8$ and $S = 4$ for our experiments on ImageNet. We consider $K = 16$ transformations in Algorithm 1, including AutoContrast, Brightness, Color, Contrast, Cutout, Equalize, Invert, Mixup, Posterize, Rotate, Sharpness, ShearX, ShearY, Solarize, TranslateX, TranslateY. See e.g. (Shorten & Khoshgoftaar, 2019) for descriptions of these transformations.

As is common in previous work, we also include a parameter to set the probability of applying a transformation in Line 4 of Algorithm 1. We set this parameter and the magnitude of each transformation randomly in a suitable range. We apply the augmentations over the entire training dataset. We report the results averaged over four random seeds.

5.2. Experimental Results

We apply Algorithm 1 on three image classification tasks (CIFAR10, CIFAR100, SVHN, and ImageNet) over several models. Table 3 summarizes the result. We highlight the comparisons to RandAugment and Adversarial AutoAugment since they dominate the other benchmark methods.

Improving classification accuracy over RandAugment. For Wide-ResNet-28-10, we find that our method outperforms RandAugment by 0.59% on CIFAR-10 and 1.24% on CIFAR-100. If we do not use Mixup, our method still outperforms RandAugment by 0.45% on CIFAR-10. For Shake-Shake and PyramidNet+ShakeDrop, our method improves the accuracy of RandAugment by 0.27% and 0.16% on CIFAR-10, respectively. For ResNet-50 on ImageNet dataset, our method achieves top-1 accuracy 79.14% which outperforms RandAugment by 1.54%.

Improving training efficiency over Adversarial AutoAugment. Our method achieves comparable accuracy to the current state-of-the-art on CIFAR-10, CIFAR-100, and ImageNet. Algorithm 1 uses additional inference cost to find the uncertain samples. And we estimate that the additional cost equals half of the training cost. However, the inference cost is 5x cheaper compared to training the adversarial network of Adversarial AutoAugment, which requires generating 8 times more samples for training.

Further improvement by increasing the number of augmented samples. Recall that Algorithm 1 contains a parameter $S$ which controls how many new labeled data we generate per training data. The results in Table 3 use $C = 4$ and $S = 1$, but we can further boost the prediction accuracy by increasing $C$ and $S$. In Table 4, we find that by setting $C = 8$ and $S = 4$, our method improves the accuracy of Adversarial AutoAugment on CIFAR-100 by 0.49% on Wide-ResNet-28-10.

5.3. Ablation Studies

Histogram of selected transformations. We examine the transformations selected by Algorithm 1 to better understand its difference compared to RandAugment. For this
### Table 3. Test accuracy (%) on CIFAR-10, CIFAR-100, and SVHN. We compare our method with default data augmentation (Baseline), AutoAugment (AA), Fast AutoAugment (Fast AA), Population Based Augmentation (PBA), RandAugment (RA), and Adversarial AutoAugment (Adv. AA). Our results are averaged over four random seeds except ImageNet experiments.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Baseline</th>
<th>AA</th>
<th>Fast AA</th>
<th>PBA</th>
<th>RA</th>
<th>Adv. AA</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFAR-10</td>
<td>Wide-ResNet-28-10</td>
<td>96.13</td>
<td>97.32</td>
<td>97.30</td>
<td>97.42</td>
<td>97.30</td>
<td><strong>98.10</strong></td>
<td>97.89% (± 0.03%)</td>
</tr>
<tr>
<td></td>
<td>Shake-Shake (26 2x96d)</td>
<td>97.14</td>
<td>98.01</td>
<td>98.00</td>
<td>97.97</td>
<td>98.00</td>
<td>98.15</td>
<td>98.27% (± 0.05%)</td>
</tr>
<tr>
<td></td>
<td>PyramidNet+ShakeDrop</td>
<td>97.33</td>
<td>98.52</td>
<td>98.30</td>
<td>98.54</td>
<td>98.50</td>
<td>98.64</td>
<td>98.66% (± 0.02%)</td>
</tr>
<tr>
<td>CIFAR-100</td>
<td>Wide-ResNet-28-10</td>
<td>81.20</td>
<td>82.91</td>
<td>82.70</td>
<td>83.27</td>
<td>83.30</td>
<td>84.51</td>
<td>84.54% (± 0.09%)</td>
</tr>
<tr>
<td>SVHN</td>
<td>Wide-ResNet-28-10</td>
<td>96.9</td>
<td>98.1</td>
<td>-</td>
<td>-</td>
<td><strong>98.3</strong></td>
<td>-</td>
<td>98.3% (± 0.03%)</td>
</tr>
<tr>
<td>ImageNet</td>
<td>ResNet-50</td>
<td>76.31</td>
<td>77.63</td>
<td>77.60</td>
<td>-</td>
<td>77.60</td>
<td><strong>79.40</strong></td>
<td>79.14%</td>
</tr>
</tbody>
</table>

**Figure 4.** Increasing the number of augmented data points per training sample can further improve accuracy.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Adv. AA</th>
<th>Ours (S = 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFAR-10</td>
<td>98.10 (±0.15%)</td>
<td><strong>98.16% (± 0.05%)</strong></td>
</tr>
<tr>
<td>CIFAR-100</td>
<td>84.51 (±0.18%)</td>
<td><strong>85.02% (± 0.18%)</strong></td>
</tr>
</tbody>
</table>

**Figure 5.** Comparing the training cost between our method, RA and Adv. AA on CIFAR-10 relative to RA. The training cost of Adv. AA is cited from the authors (Zhang et al., 2020).

### 5.4. Extension to Text Augmentations

While we have focused on image augmentations throughout the paper, we can also use our ideas to text augmentations. We extend Algorithm 1 to a sentiment analysis task as follows. We choose BERT\textsubscript{LARGE} as the baseline model, which is a 24 layer transformer network from (Devlin et al., 2018). We apply our method to three augmentations: back-translation (Yu et al., 2018), switchout (Wang et al., 2018), and word replace (Xie et al., 2019).

**Dataset.** We use the Internet movie database (IMDb) with 50,000 movie reviews. The goal is to predict whether the sentiment of the review is positive or negative.

**Comparison methods.** We compare with pre-BERT SoTA, BERT\textsubscript{LARGE}, and unsupervised data augmentation (UDA) (Xie et al., 2019). UDA uses BERT\textsubscript{LARGE} initialization and training on 20 supervised examples and DBPedia (Lehmann et al., 2015) as an unsupervised source.

**Results.** We find that our method achieves test accuracy 95.96%, which outperforms all the other methods by at least 0.28%. For reference, the result of using Pre-BERT SoTA is 95.68%. The result of using BERT\textsubscript{LARGE} is 95.22%. The result of using UDA is 95.22%.

### 6. Related Work

**Image augmentations.** We describe a brief summary and refer interested readers to the excellent survey by (Shorten & Khoshgoftaar, 2019) for complete references.

Data augmentation has become a standard practice in computer vision such as image classification tasks. First, individual transformations such as horizontal flip and mixup have shown improvement over strong vanilla models. Beyond individual transformations, one approach to search for compositions of transformations is to train generative adversarial networks to generate new images as a form of data augmentation (Sixt et al., 2018; Laine & Aila, 2016; Odena, 2016; Gao et al., 2018). Another approach is to use reinforcement learning based search methods (Hu et al., 2019). The work of Cubuk et al. (2018) searches for the augmentation schemes on a small surrogate dataset. While this idea reduces the search cost, it was shown that using a small surrogate dataset results in sub-optimal augmentation policies (Cubuk et al., 2019).

The work of Kuchnik & Smith (2018) is closely related to ours since they also experiment with the idea of uncertainty-
based sampling. Their goal is different from our work in that they use this idea to find a representative sub-sample of the training dataset that can still preserve the performance of applying augmentation policies. Recently, the idea of mixing data has been applied to semi-supervised learning by mixing feature representations as opposed to the input data (Berthelot et al., 2019).

**Theoretical studies.** Dao et al. (2019) propose a kernel theory to show that label-invariant augmentations are equivalent to transforming the kernel matrix in a way that incorporates the prior of the transformation. Chen et al. (2019) use group theory to show that incorporating the label-invariant property into an empirical risk minimization framework reduces variance.

Our theoretical setup is related to Xie et al. (2020); Raghu-nathan et al. (2020), with several major differences. First, in our setting, we assume that the label of an augmented data is generated from the training data, which is deterministic. In their setting, the label of an augmented data includes new information because the random noise is freshly drawn. Second, we consider the ridge estimator as opposed to the minimum norm estimator, since the ridge estimator includes an $\ell_2$ regularization which is commonly used in practice. Finally, it would be interesting to extend our theoretical setup beyond linear settings (e.g. (Li et al., 2018; Zhang et al., 2019; Montanari et al., 2019)).

### 7. Conclusions and Future Work

In this work, we studied the theory of data augmentation in a simplified over-parametrized linear setting that captures the need to add more labeled data as in image settings, where there are more parameters than the number of data points. Despite the simplicity of the setting, we have shown three novel insights into three categories of transformations. We verified our theoretical insights on MNIST. And we proposed an uncertainty-based sampling scheme which outperforms random sampling. We hope that our work can spur more interest in developing a better understanding of data augmentation methods. Below, we outline several questions that our theory cannot yet explain.

First, one interesting future direction is to further uncover the mysterious role of mixup (Zhang et al. 17). Our work has taken the first step by showing the connection between mixup and regularization. Meanwhile, Table 7 (in Appendix) shows that mixup can reduce the model error score (bias) on CIFAR-10. Our theory does not explain this phenomenon because our setup implicit assumes a single class (the linear model $\beta$) for all data. We believe that extending our work to a more sophisticated setting, e.g. mixed linear regression model, is an interesting direction to explain the working of mixup augmentation over multiple classes.

Second, it would be interesting to consider the theoretical benefit of our proposed uncertainty-based sampling algorithm compared to random sampling, which can help tighten the connection between our theory and the proposed algorithm. We would like to remark that addressing this question likely requires extending the models and tools that we have developed in this work. Specifically, one challenge is how to come up with a data model that will satisfy the label-invariance property for a large family of linear transformations. We leave these questions for future work.

### Acknowledgements.

We gratefully acknowledge the support of DARPA under Nos. FA86501827865 (SDH) and FA86501827882 (ASED); NIH under No. U54EB020405 (Mobilize), NSF under Nos. CCF1763315 (Beyond Sparsity), CCF1563078 (Volume to Velocity), and 1937301 (RTML); ONR under No. N000141712266 (Unifying Weak Supervision); the Moore Foundation, NXP, Xilinx, LETI-CEA, Intel, IBM, Microsoft, NEC, Toshiba, TSMC, ARM, Hitachi, BASF, Accenture, Ericsson, Qualcomm, Analog Devices, the Okawa Foundation, American Family Insurance, Google Cloud, Swiss Re, the HAI-AWS Cloud Credits for Research program, and members of the Stanford DAWN project: Teradata, Facebook, Google, Ant Financial, NEC, VMWare, and Infosys. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views, policies, or endorsements, either expressed or implied, of DARPA, NIH, ONR, or the U.S. Government.

Gregory Valiant’s contributions were supported by NSF awards 1804222, 1813049 and 1704417, DOE award DESC0019205 and an ONR Young Investigator Award. Our experiments are partly run on Stanford University’s SOAL cluster hosted in the Department of Management Science and Engineering (cf. https://5harad.com/soal-cluster/).

### References


We describe the following lemma, which tracks the change of bias and variance for augmenting why mixup helps improve performance in image classification tasks.

The Sherman-Morrison formula. Suppose \( D \in \mathbb{R}^{d \times d} \) is an invertible square matrix and \( u, v \in \mathbb{R}^d \) are column vectors. Then \( X + uv^\top \) is invertible if and only if \( 1 + u^\top X v \neq 0 \). In this case,

\[
(X + uv^\top)^{-1} = X^{-1} - A^{-1}uv^\top A^{-1} \frac{1}{1 + u^\top X A^{-1}v}.
\]

A.1. Proof of Theorem 3.1

We describe the following lemma, which tracks the change of bias and variance for augmenting \((X,Y)\) with \((z,y)\).

Lemma A.1. Let \( X^\top X = UD U^\top \) denote the singular vector decomposition of \( X^\top X \). Denote by \( \varepsilon^{\text{aug}} = y^{\text{aug}} - z^\top \beta \). In the setting of Theorem 3.1, we have that

\[
\text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}_{\text{aug}}) \geq \frac{(2\lambda(n+1) - (1-2\lambda)\|z\|^2)\langle z, \beta \rangle^2}{\lambda^2 n^2 + \lambda^2 d^2 + 2n \lambda d + \|z\|^2 \langle z, \beta \rangle^2},
\]

\[ \text{var}(\hat{\beta}) - \text{var}(\hat{\beta}_{\text{aug}}) \geq 2 \mathbb{E}_{\varepsilon} \left[ (\varepsilon^{\text{aug}} - X^{\text{aug}} \varepsilon^{\text{aug}} + (n+1)\lambda \text{Id})^{-1} X^\top \varepsilon \right] - \mathbb{E} \left[ \varepsilon^{\text{aug}} \| (X^{\text{aug}} X^{\text{aug}} + (n+1)\lambda \text{Id})^{-1} z \| \right]^2.
\]

Proof. The reduction of bias is given by

\[
\text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}_{\text{aug}}) = \| (X^\top X + n \lambda \text{Id})^{-1} X^\top X \beta - \beta \|^2 - \| (X^{\text{aug}} X^{\text{aug}} + (n+1)\lambda \text{Id})^{-1} X^{\text{aug}} X^{\text{aug}} \beta - \beta \|^2.
\]

Denote by \( K_{n+1} = (X^\top X/n + \lambda \text{Id})^{-1} \) and \( K_n = (X^\top X/n + \lambda \text{Id})^{-1} \). We observe that

\[
\left( \frac{X^{\text{aug}} X^{\text{aug}}}{n+1} + \lambda \text{Id} \right)^{-1} = \left( \frac{X^\top X}{n+1} + \lambda \text{Id} + \frac{zz^\top}{n+1} \right)^{-1}.
\]

\[
= K_{n+1} - \frac{1}{n+1} \cdot K_{n+1} \frac{zz^\top}{n+1} K_{n+1} \quad (\text{because } P_X z = 0)
\]

\[
= K_{n+1} - U \Delta U^\top - \frac{(n+1)\lambda^2 zz^\top}{1 + \|z\|^2/n+1},
\]
where we use $\Delta \in \mathbb{R}^{n \times n}$ to denote a diagonal matrix with the $i$-th diagonal entry being $\frac{1}{n(n+1)}(D_{i,i}/\var{\lambda}(D_{i,i}/(n+1)+\lambda)$, i.e. $\Delta = (\frac{1}{n+\lambda} - \frac{1}{n+\lambda})$. From this we infer that bias($\hat{\beta}$) - bias($\hat{\beta}_{aug}$) is equal to

$$
\lambda^2 \left( 2(K_{n,\beta}, U\Delta U^T + \frac{1}{n+1}\lambda^2 z^T z) - \left\| \left( U\Delta U^T + \frac{1}{n+1}\lambda^2 z^T z \right) \beta \right\|^2 \right)
\quad = \frac{2(z, \beta)^2}{\lambda(n+1 + \|z\|^2)} + \lambda^2 \left( 2(\frac{1}{D} - \frac{1}{\lambda}) U\Delta U^T \beta - \|U\Delta U^T \beta\|^2 \right) - \frac{\|z\|^2(z, \beta)^2}{\lambda^2(n+1 + \|z\|^2)^2},
$$

where we again use the fact that $U^T z = 0$. We note that for large enough $n$, $\frac{1}{D+\lambda} \Delta$ strictly dominates $\Delta^2$. Hence we conclude that

$$
\text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}_{aug}) \geq \frac{(2\lambda(n+1) - (1 - 2\lambda)\|z\|^2)(z, \beta)^2}{\lambda^2(n+1 + \|z\|^2)^2},
$$

(12)

which proves equation (7). For the change of variance, We have that

$$
\text{var}(\hat{\beta}) - \text{var}(\hat{\beta}_{aug}) = \mathbb{E}_E \left[ \| (X^T X + n\lambda I)^{-1} X^T \varepsilon \|^2 \right] - \mathbb{E}_E \left[ \| (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-1} X_{aug}^T \varepsilon_{aug} \|^2 \right]
\quad = \sigma^2 \cdot \text{Tr} \left[ ((X^T X + n\lambda I)^{-2} - (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-2}) X^T X \right]
\quad + 2 \mathbb{E}_E ((z, \varepsilon_{aug})^2, (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-1} X^T \varepsilon)^2 - \mathbb{E}_E \left[ \varepsilon_{aug}^2 \right] \| (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-1} z \|^2
\quad \geq 2 \mathbb{E}_E ((z, \varepsilon_{aug})^2, (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-1} X^T \varepsilon)^2 - \mathbb{E}_E \left[ \varepsilon_{aug}^2 \right] \| (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-1} z \|^2.
$$

(13)

Hence equation (8) is proved by noting that equation (13) is positive. This is because $(X^T X + n\lambda I)^{-2} - (X_{aug}^T X_{aug} + (n+1)\lambda I)^{-2}$ is PSD. And the trace of the product of two PSD matrices is always positive. \hfill \Box

Based on Lemma A.1, we can prove Theorem 3.1.

\textbf{Proof of Theorem 3.1.} We note that

$$
e(\hat{\beta}) - e(\hat{\beta}_{aug}) = \text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}_{aug}) + \text{var}(\hat{\beta}) - \text{var}(\hat{\beta}_{aug}).
$$

The change of bias has been given by equation (7). For equation (8), we note that $z$ is orthogonal to $(X_{aug}^T X_{aug} + \lambda I)^{-1} X^T$. Hence the first term is zero. The second terms simplifies to

$$
- \frac{\|z\|^2}{\lambda^2(n+1)^2} \mathbb{E}_E \left[ \varepsilon_{aug}^2 \right].
$$

(14)

For $\varepsilon_{aug}$, denote by $\varepsilon_{y} = y - \beta^T \beta$, we note that $\varepsilon_{aug}$ is equal to $\varepsilon_{y} - \text{Diag} \left[ (X^T)^{T} F x \right] \varepsilon$, Hence

$$
\mathbb{E}_E \left[ \varepsilon_{aug}^2 \right] \leq 2 \mathbb{E}_E \left[ \varepsilon_{y}^2 \right] + 2 \mathbb{E}_E \left[ \text{Diag} \left[ (X^T)^{T} (x - z) \right] \varepsilon \right]
\quad = 2\sigma^2 + 2\sigma^2 \text{Diag} \left[ (X^T)^{T} F x \right]^2
\quad \leq 2\sigma^2 (1 + \frac{\|P^* F x\|^2}{\mu_{\min}(X)^2}).
$$

Combined with equation (14) and equation (7), we have proved equation (2).

For equation (3), by plugging in the assumption that $\|z\|^2 = o(n)$ and $(\frac{(z, \beta)^2}{\|z\|^2}) \geq (\log n) \cdot (1 + \frac{\|P^* F x\|^2}{\mu_{\min}(X)^2})\sigma^2/(\lambda n)$ into equation (2), we have that

$$
e(\hat{\beta}) - e(\hat{\beta}_{aug}) \geq \frac{2\lambda(n+1) - (1 - 2\lambda)\|z\|^2 - 10\log n}{\lambda^2(n+1 + \|z\|^2)}(z, \beta)^2 \geq 2(1 + o(1)) \frac{(z, \beta)^2}{\lambda n}.
$$
The proof of the above result follows by repeatedly applying Theorem 3.1. The details are omitted.

**Lemma A.3.** Let $\Delta = \text{mixup transformation}, x^\hat{\beta}$ denote a sequence of data points obtained via label-invariant transformations from $(X,Y)$. Denote by $(X_0,Y_0) = (X,Y)$. For $i = 1, \ldots, t$, let $z_i = P^\perp_{X_i} x^\text{aug}_i$ and $y^\text{aug}_i = y_i + \text{Diag} [(X_i^\top)^\perp x^\text{aug}_i] Y_i$. Suppose we augment $(X_{i-1}, Y_{i-1})$ with $(z_i, y^\text{aug}_i)$. Let $(X_i, Y_i) \in (\mathbb{R}^{(n+i) \times p}, \mathbb{R}^{n+i})$ denote the augmented dataset.

Suppose that $\lambda < 1/4$ is a small fixed constant. Let $t = O(n)$ and $\|z_i\|^2 = o(n)$, for $i = 1, \ldots, t$. Under the assumption that $\frac{(z_i, \beta)^2}{\|z_i\|^2} \geq (1 + \frac{\|P_{X_i} x^\text{aug}_i\|^2}{\min_{X_i} \|X_i\|^2}) \sigma^2 / (\lambda(n + i))$, we have

$$e(\hat{\beta}(X,Y)) - e(\hat{\beta}(X_i, Y_i)) \geq \sum_{i=1}^t \frac{(z_i, \beta)^2}{\lambda n}.$$

The proof of the above result follows by repeatedly applying Theorem 3.1. The details are omitted.

**A.2. Proof of Theorem 3.3**

Similar to the proof of Theorem 3.1, we also track the change of the bias and the variance of $\hat{\beta}$. The difference is that for the mixup transformation, $x^\text{aug}$ lies in the row span of $X$. The following Lemma tracks the change of bias and variance in this setting.

**Lemma A.3.** Let $\varepsilon^\text{mixup} = \alpha \varepsilon_i + (1 - \alpha) \varepsilon_j$. In the setting of Theorem 3.3, we have that

$$\text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}^\text{aug}) \leq \frac{2\lambda(1 + 1 - 2 \lambda) \|z\|^2 (z, \beta)^2}{\lambda^2 (n + 1 + \|z\|^2)} + O \left( \frac{\text{poly}(\gamma, 1/\lambda)}{n^2} \right).$$

For the change of variance, from the calculation of equation (13), we have

$$\text{var}(\hat{\beta}) - \text{var}(\hat{\beta}^\text{aug}) \leq \sigma^2 \cdot \text{Tr} \left[ ((X^\top X + n \lambda \text{Id})^{-2} - (X^\text{aug}^\top X^\text{aug} + (n + 1) \lambda \text{Id})^{-2}) X^\top X \right] \leq \sigma^2 \cdot \text{Tr} \left[ ((X^\top X + n \lambda \text{Id})^{-2} - (X^\top X + (n + 1) \lambda \text{Id})^{-2}) X^\top X \right] + O \left( \frac{\text{poly}(\gamma, 1/\lambda)}{n^2} \right).$$

Therefore, we have shown that

$$e(\hat{\beta}) - e(\hat{\beta}^\text{aug}) \leq 2(1 + o(1)) \frac{(z, \beta)^2}{\lambda n} + O \left( \frac{\text{poly}(\gamma, 1/\lambda)}{n^2} \right).$$

Hence the proof of the theorem is complete. \qed

**Extension to Adding Multiple Data Points.** We can also extend Theorem 3.1 to the case of adding multiple transformed data points. The idea is to repeatedly apply Theorem 3.1 and equation (3). We describe the result as a corollary as follows.

**Corollary A.2.** In the setting of Theorem 3.1. Let $(x^\text{aug}_1, y^\text{aug}_1), (x^\text{aug}_2, y^\text{aug}_2), \ldots, (x^\text{aug}_t, y^\text{aug}_t)$ denote a sequence of data points obtained via label-invariant transformations from $(X,Y)$. Denote by $(X_0,Y_0) = (X,Y)$. For $i = 1, \ldots, t$, let $z_i = P^\perp_{X_i} x^\text{aug}_i$ and $y^\text{aug}_i = y_i^\text{aug} - \text{Diag} [(X_i^\top)^\perp x^\text{aug}_i] Y_i$. Suppose we augment $(X_{i-1}, Y_{i-1})$ with $(z_i, y^\text{aug}_i)$. Let $(X_i, Y_i) \in (\mathbb{R}^{(n+i) \times p}, \mathbb{R}^{n+i})$ denote the augmented dataset.

Suppose that $\lambda < 1/4$ is a small fixed constant. Let $t = O(n)$ and $\|z_i\|^2 = o(n)$, for $i = 1, \ldots, t$. Under the assumption that $\frac{(z_i, \beta)^2}{\|z_i\|^2} \geq (1 + \frac{\|P_{X_i} x^\text{aug}_i\|^2}{\min_{X_i} \|X_i\|^2}) \sigma^2 / (\lambda(n + i))$, we have

$$e(\hat{\beta}(X,Y)) - e(\hat{\beta}(X_i, Y_i)) \geq \sum_{i=1}^t \frac{(z_i, \beta)^2}{\lambda n}.$$
From equation (9) and (10), we have that the change of bias is equal to
\[
\text{bias}(\hat{\beta}) - \text{bias}(\hat{\beta}^{\text{mixup}}) = 2\lambda^2 \left( (K_n, \beta) \left( \frac{U \Delta U^T}{n(n+1)} + \frac{Z}{n+1} \right) \beta \right) - \lambda^2 \left( \frac{U \Delta U^T}{n(n+1)} + \frac{Z}{n+1} \right) \beta \left\| \beta \right\|^2 \\
= \lambda^2 \beta^T U \left( 2 \left( \frac{D}{n+1} \right)^{-1} \frac{\Delta}{n(n+1)} - \frac{\Delta^2}{n^3(n+1)^2} - 2 \frac{1}{n+1} \frac{1}{n+1} \frac{U^T x^{\text{aug}} x^{\text{aug}}^T X}{n+1} \left( \frac{U^T x^{\text{aug}} x^{\text{aug}}^T X}{n+1} \right) \right) U^T \beta \\
+ \frac{2\lambda^2}{n+1} \left( K_n, Z \beta \right) - \frac{\lambda^2}{n+1} \left\| Z \beta \right\|^2
\]
(17)

For equation (17), we have used the fact that \(P_X z = 0\). We observe that for large enough \(n\), equation (17) is always positive, since the negative terms are both on the order of \(O(\frac{1}{n^2})\). Hence we focus on equation (18). First, we observe that
\[
\langle K_n \beta, Z \beta \rangle = \beta^T K_n K_{n+1} x^{\text{aug}} x^{\text{aug}}^T K_{n+1} \beta - \frac{C}{C+1} \langle K_n \beta, K_{n+1} x^{\text{aug}} x^{\text{aug}}^T K_{n+1} \beta \rangle \\
= \beta^T U \left( \frac{D}{n+1} \right)^{-1} \frac{1}{\lambda} \left( D + \lambda \right)^{-1} U^T x^{\text{aug}} x^{\text{aug}}^T U \left( \frac{D}{n+1} + \lambda \right)^{-1} U^T \beta - \frac{C}{C+1} \langle K_n \beta, K_{n+1} x^{\text{aug}} x^{\text{aug}}^T K_{n+1} \beta \rangle
\]
(18)

We observe that
\[
\frac{C}{C+1} \left| \langle K_n \beta, K_{n+1} x^{\text{aug}} x^{\text{aug}}^T K_{n+1} \beta \rangle \right| \leq \frac{1}{n+1} \left\| \beta \right\|^2 \left\| x^{\text{aug}} \right\|^2 \frac{1}{\lambda^2} \leq \frac{1}{n+1} \frac{\left\| \beta \right\|^2 \gamma^4}{\lambda^4}
\]
\[
\left\| Z \beta \right\| \leq \frac{1}{\lambda^2} \cdot \left\| \beta \right\| \cdot \left\| x^{\text{aug}} \right\|^2 \leq \frac{\left\| \beta \right\|^2 \gamma^2}{\lambda^4}.
\]
Hence (15) is proved.

Next, denote by \(K_{\text{aug}} = (X^{\text{aug}}^T X^{\text{aug}} + \lambda \Id)^{-1}\). We have that the change of variance is given as
\[
\text{var}(\hat{\beta}) - \text{var}(\hat{\beta}^{\text{mixup}}) = \sigma^2 \cdot \left| \left( \begin{array}{c} n \end{array} \right) \right| \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right) - \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right)
\]
\[
\geq \sigma^2 \cdot \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right) - \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right) \left( \begin{array}{c} n \end{array} \right)
\]
because \(K^2 - K_{\text{aug}}^2\) is PSD and the trace of the product of two PSD matrices is always positive. Next, recall that that \(\varepsilon^{\text{aug}} = \alpha \varepsilon_i + (1-\alpha) \varepsilon_j\), we have
\[
\mathbb{E}_{\varepsilon} \left[ X^{\text{aug}}^T \varepsilon^{\text{aug}} \varepsilon^{\text{aug}}^T X^{\text{aug}} \right] = \sigma^2 \cdot \left( (\alpha^2 + (1-\alpha)^2) \cdot \varepsilon^T + 2\alpha^{\text{aug}} x_i^{\text{aug}} + 2(1-\alpha) x_j^{\text{aug}} + X^T X \right)
\]
\[
= \sigma^2 \cdot \left( (\alpha^2 + (1-\alpha)^2 + 2) \cdot x^{\text{aug}} + X^T X \right).
\]
(19)

Hence equation (16) is proved.

Based on Lemma A.3, we can finish the proof of Theorem 3.3.

**Proof of Theorem 3.3.** We recall that \(z = \alpha x_i + (1-\alpha)x_j\), where \(x_i, x_j\) are sampled uniformly at random from \(X\). Therefore,
\[
\mathbb{E}_{x_i, x_j} \left[ x^{\text{aug}} x^{\text{aug}}^T \right] = \frac{\alpha^2 + (1-\alpha)^2}{n} X^T X + \frac{2\alpha(1-\alpha)}{n} \sum_{1 \leq i \leq n} x_i \left( \sum_{j \neq i} x_j \right)
\]
\[
= \frac{\alpha^2 + (1-\alpha)^2}{n} X^T X + \frac{2\alpha(1-\alpha)}{n} \left( \sum_{i=1}^n x_i \left( \sum_{i=1}^n x_i^T \right) - X^T X \right)
\]
\[
= \frac{(1-2\alpha)^2}{n} X^T X,
\]
where in the last line we used the assumption that $\sum_{i=1}^n x_i = 0$. For $\alpha$ sampled from a Beta distribution with parameters $a, b$, we have $\mathbb{E}_\alpha \left[ (1 - 2\alpha)^2 \right] = 1 - \frac{4ab(a+b)}{(a+b)^2(a+b+1)} = \frac{(a-b)^2(a+b)}{(a+b)^2(a+b+1)} + \frac{1}{a+b+1}$ which is a constant when $a, b$ are constant values. Denote this value by $c$. By plugging in the above equation back to equation (15), we have that in expectation over the randomness of $\alpha, x_i, x_j$, the change of bias is at least

$$bias(\hat{\beta}) - bias(\hat{\beta}^{\text{mixup}}) \geq \frac{2\lambda^2 c}{n(n+1)} \beta^\top U \left( \frac{D}{n+1} + \lambda \right)^2 \frac{D}{n+1} U^\top \beta - \frac{3\|\beta\|^2 \gamma^4}{\lambda^2 (n+1)^2} \geq \frac{2\lambda^2 c}{(\gamma + \lambda)^3 (n+1)} \frac{||X\beta||^2}{n} - \frac{3\|\beta\|^2 \gamma^4}{\lambda^2 (n+1)^2}.$$

Similarly, using equation (16), we obtain that in expectation over the randomness of $z$, the change of variance is at least

$$\text{var}(\hat{\beta}) - \text{var}(\hat{\beta}^{\text{mixup}}) \geq -3\frac{\sigma^2 c}{n} \cdot \text{Tr} \left[ \left( X^\top X + n\lambda \text{Id} \right)^{-1} X^\top X \left( X^\top X + n\lambda \text{Id} \right)^{-1} \right] = -3\frac{\sigma^2 c}{\lambda^2 n^2} ||X||^2 \geq -3\frac{\sigma^2 c \gamma^2}{\lambda^2 n^2}.$$

In summary, when $n$ is large enough, e.g. for

$$n \geq \frac{6(\gamma + \lambda)^3}{\lambda^4} \max \left( \frac{\|\beta\|^2 \gamma^4}{c}, \sigma^2 \gamma^2 \right),$$

we conclude that

$$e(\hat{\beta}) - e(\hat{\beta}^{\text{mixup}}) \geq \frac{\lambda^2 c ||X\beta||^2}{(\gamma + \lambda)^3 n^2} \geq \frac{\lambda^2 ||X\beta||^2}{\gamma^3 n^2}.$$

**Discussions.** Our result on the mixup augmentations opens up several immediate open questions. First, our setting assumes that there is a single linear model $\beta$ for all data. An interesting direction is to extend our results to a setting with multiple linear models. This extension can better capture the multi-class prediction problems that arise in image classification tasks.

Second, our result also deals with adding a simple mixup sample. The limitation is that adding the mixup sample violates the assumption that $\sum_{i=1}^n x_i = 0$ we make for the proof to go through. However, one would expect that the assumption is still true in expectation after adding the mixup sample. Formally establishing the result is an interesting question.

**A.3. Proof of Corollary 3.4**

*Proof of Corollary 3.4.* The proof is by applying equation (3) over $z_1 + z_2$ and $z_1$ twice. The result follows by adding up results from the two. The details are omitted.

**A.4. The Minimum Norm Estimator**

In addition to the ridge estimator, the minimum norm estimator has also been studied in the over-parametrized linear regression setting (Bartlett et al., 2019; Xie et al., 2020). The minimum norm estimator is given by solving the following.

$$\min_{w \in \mathbb{R}^p} \|w\|^2 \quad \text{s.t.} \quad Xw = Y.$$

It is not hard to show that the solution to the above is given as $\hat{\beta} = (X^\top X)^\dagger X^\top Y$. We have focused on the ridge estimator since it is typically the case in practice that an $l_2$-regularization is added to the objective. In this part, we describe the implications of our results for the minimum norm estimator.
For this case, we observe that
\[ \mathbb{E}_\varepsilon [\hat{\beta}] - \beta = (X^\top X)^\dagger X^\top X \beta - X = -P_X^\perp \beta, \]
where \( P_X^\perp \) is the projection orthogonal to \( X^\top X \). Hence we can simplify the bias term to be \( \beta^\top P_X^\perp \beta \). The variance term is \( \text{Tr}(X^\top X)^\dagger \).

**Dealing with pseudoinverse.** We need the following tools for rank-one updates on matrix pseudoinverse. Suppose \( X \in \mathbb{R}^{d \times d} \) is not invertible and \( u \in \mathbb{R}^d \) are column vectors. Let \( v = P_X u \) denote the projection of \( u \) onto the subspace of \( X \). Let \( s = P_X^\perp u \) denote the projection of \( u \) orthogonal to \( X \). Suppose that \( 1 + u^\top X^\top u \neq 0 \) and \( s, v \) are nonzero. In this case,
\[ \begin{align*}
(X + uu^\top)^\dagger &= X^\dagger - X^\dagger vs^\top - s^\top v^\top X^\dagger + (1 + u^\top X^\top u) s^\dagger s^\top T \\
&= X^\dagger - X^\dagger us^\top - s^\top u^\top X^\dagger + (1 + u^\top X^\top u) s^\dagger s^\top T.
\end{align*} \tag{20} \]

If \( s \) is zero, in other words \( u \) is in the row span of \( X \), then
\[ (X + uu^\top)^\dagger = X^\dagger - \frac{X^\dagger uu^\top X^\dagger}{1 + u^\top X^\top u}. \]

The proof of these identities can be found in (Riedel, 1992).

**Label-invariant transformations.** When \( \sigma = 0 \), i.e. there is no label in the labels, we can get a result qualitatively similar to Theorem 3.1 for the minimum norm estimator. This is easy to see because the bias term is simply \( \beta^\top P_X^\perp \beta \). When we add \( z \) which is orthogonal to the span of \( X \), then we get that
\[ P_{X^{\text{aug}}}^\perp = P_X^\perp - \frac{zz^\top}{\|z\|^2}. \]

Hence the bias of \( \hat{\beta} \) reduces by \( \frac{(z, \beta)^2}{\|z\|^2} \).

When \( \sigma \neq 0 \), the variance of \( \hat{\beta} \) can increase at a rate which is proportional to \( 1/\|z\|^2 \). This arises when we apply (20) on \( (X^\top X + zz^\top)^\dagger \). In Theorem 3.1, we can circumvent the issue because the ridge estimator ensures the minimum singular value for \( P_X^\perp \) is at least \( \lambda \).

**The mixup transformations.** For the minimum norm estimator, we show that adding a mixup sample always increases the estimation error for \( \beta \). This is described as follows.

**Proposition A.4.** Let \( X_{\text{aug}} \) and \( Y_{\text{aug}} \) denote the augmented data after adding \( (x_{\text{aug}}, y_{\text{aug}}) \) to \( (X, Y) \). Then for the minimum norm estimator, we have that: a) the bias is unchanged; b) the variance increases, for any constant \( \alpha \in (0, 1) \) which does not depend on \( n \).

**Proof.** For Claim a), we note that since \( P_{X_{\text{aug}}}^\perp x_{\text{aug}} = 0 \), we have \( P_{X_{\text{aug}}}^\perp = P_X^\perp \). Hence, the bias term stays unchanged after adding \( (x_{\text{aug}}, y_{\text{aug}}) \).

For Claim b), we note that the variance of \( \hat{\beta} \) for the test error is given by
\[ \text{Tr} \left[ (X_{\text{aug}}^\top X_{\text{aug}})^\dagger (X_{\text{aug}}^\top X_{\text{aug}})^\dagger X_{\text{aug}}^\top x_{\text{aug}} x_{\text{aug}}^\top X_{\text{aug}} \right] \]
Taking the expectation over \( \varepsilon \), we have (c.f. equation (19))
\[ \mathbb{E}_\varepsilon \left[ X_{\text{aug}}^\top x_{\text{aug}} x_{\text{aug}}^\top X_{\text{aug}} \right] = \sigma^2 \cdot \left( \alpha^2 + (1 - \alpha)^2 + 2 \right) x_{\text{aug}}^\top x_{\text{aug}}^\top X \]
Meanwhile, for \( (X_{\text{aug}}^\top X_{\text{aug}})^\dagger \), we use the Sherman-Morrison formula to decompose the change of the rank-1 update \( x_{\text{aug}}^\top x_{\text{aug}} \).
Since \( P_X^\perp x_{\text{aug}} = 0 \) and \( x_{\text{aug}}^\top K x_{\text{aug}} \leq \|x_{\text{aug}}\|^2 / n < 1 \). Denote by \( K = (X^\top X)^\dagger \), we have
\[ (X_{\text{aug}}^\top X_{\text{aug}})^\dagger = K - \frac{K x_{\text{aug}} x_{\text{aug}}^\top K}{1 + x_{\text{aug}}^\top K x_{\text{aug}}} \]
To sum up, we have that

$$
\mathbb{E} \left[ \text{Tr} \left[ (X_{\text{aug}}^\top X_{\text{aug}})^\dagger (X_{\text{aug}}^\top X_{\text{aug}}) X_{\text{aug}}^\top \epsilon_{\text{aug}} \epsilon_{\text{aug}}^\top X_{\text{aug}} \right] \right] = \sigma^2 \text{Tr} [K] + (\alpha^2 + (1 - \alpha)^2) \text{Tr} [K X_{\text{aug}} x_{\text{aug}}^\top] \cdot (1 + O(\frac{1}{n}))
$$

Hence the variance of the minimum norm estimator increases after adding the mixup sample.

B. Supplementary Materials for Section 4

We present a full list of results using our proposed metrics to study label-invariant transformations on MNIST. Then, we provide an in-depth study of the data points corrected by applying the rotation transformation. Finally, we show that we can get a good approximation of our proposed metrics by using 3 random seeds. The training details are deferred to Appendix C.

Further results on label-invariant transformations. For completeness, we also present a full list of results for label-invariant transformations on MNIST in Table 4. The descriptions of these transformations can be found in the survey of (Shorten & Khoshgoftaar, 2019).

<table>
<thead>
<tr>
<th>Transform</th>
<th>Avg. Acc.</th>
<th>Error score</th>
<th>Instability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>98.08%</td>
<td>1.52%</td>
<td>0.95%</td>
</tr>
<tr>
<td>Invert</td>
<td>97.29%</td>
<td>1.85%</td>
<td>1.82%</td>
</tr>
<tr>
<td>VerticalFlip</td>
<td>97.30%</td>
<td>1.84%</td>
<td>1.82%</td>
</tr>
<tr>
<td>HorizontalFlip</td>
<td>97.37%</td>
<td>1.83%</td>
<td>1.72%</td>
</tr>
<tr>
<td>Blur</td>
<td>97.90%</td>
<td>1.62%</td>
<td>1.24%</td>
</tr>
<tr>
<td>Solarize</td>
<td>97.96%</td>
<td>1.51%</td>
<td>1.27%</td>
</tr>
<tr>
<td>Brightness</td>
<td>98.00%</td>
<td>1.69%</td>
<td>1.05%</td>
</tr>
<tr>
<td>Posterize</td>
<td>98.04%</td>
<td>1.59%</td>
<td>1.12%</td>
</tr>
<tr>
<td>Contrast</td>
<td>98.08%</td>
<td>1.61%</td>
<td>0.93%</td>
</tr>
<tr>
<td>Color</td>
<td>98.10%</td>
<td>1.59%</td>
<td>0.88%</td>
</tr>
<tr>
<td>Equalize</td>
<td>98.12%</td>
<td>1.53%</td>
<td>0.93%</td>
</tr>
<tr>
<td>AutoContrast</td>
<td>98.17%</td>
<td>1.50%</td>
<td>0.87%</td>
</tr>
<tr>
<td>Sharpness</td>
<td>98.17%</td>
<td>1.45%</td>
<td>0.92%</td>
</tr>
<tr>
<td>Smooth</td>
<td>98.18%</td>
<td>1.47%</td>
<td>0.99%</td>
</tr>
<tr>
<td>TranslateY</td>
<td>98.19%</td>
<td>1.27%</td>
<td>1.13%</td>
</tr>
<tr>
<td>Cutout</td>
<td>98.31%</td>
<td>1.43%</td>
<td>0.86%</td>
</tr>
<tr>
<td>TranslateX</td>
<td>98.37%</td>
<td>1.21%</td>
<td>1.00%</td>
</tr>
<tr>
<td>ShearY</td>
<td>98.54%</td>
<td>1.17%</td>
<td>0.85%</td>
</tr>
<tr>
<td>ShearX</td>
<td>98.59%</td>
<td>1.00%</td>
<td>0.84%</td>
</tr>
<tr>
<td>RandomCropping</td>
<td>98.61%</td>
<td>1.01%</td>
<td>0.88%</td>
</tr>
<tr>
<td>Rotation</td>
<td>98.65%</td>
<td>1.08%</td>
<td>0.77%</td>
</tr>
</tbody>
</table>

Table 4. Measuring the intrinsic error and instability scores of label-invariant transformations on MNIST. The results are obtained using 9 random seeds.

Next we describe the details regarding the experiment on rotations. Recall that our goal is to show that adding rotated data points provides new information. We show the result by looking at the data points that are corrected after adding the rotated data points. Our hypothesis is that the data points that are corrected should be wrong “with high confidence” in the baseline model, as opposed to being wrong “with marginal confidence”.

Here is our result. Among the 10000 test data points, we observe that there are 57 data points which the baseline model predicts wrong but adding rotated data corrects the prediction. And there are 18 data points which the baseline model predicts correctly but adding rotated data. Among the 57 data points, the average accuracy of the baseline model over the 9 random seeds is 19.50%. Among the 18 data points, the average accuracy of the augmented model is 29.63%. The result confirms that adding rotated data corrects data points whose accuracies are low (at 19.50%).

Efficient estimation. We further observe that on MNIST, three random seeds are enough to provide an accurate estimation of
On the Generalization Effects of Linear Transformations in Data Augmentation

<table>
<thead>
<tr>
<th>Baseline</th>
<th>HorizontalFlip</th>
<th>Contrast</th>
<th>Cutout</th>
<th>TranslateY</th>
<th>ShearX</th>
<th>RandomCropping</th>
<th>Rotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 seeds</td>
<td>1.75%</td>
<td>1.83%</td>
<td>1.61%</td>
<td>1.43%</td>
<td>1.27%</td>
<td>1.00%</td>
<td>1.01%</td>
</tr>
<tr>
<td>3 seeds</td>
<td>1.72%</td>
<td>2.13%</td>
<td>1.78%</td>
<td>1.54%</td>
<td>1.49%</td>
<td>1.10%</td>
<td>1.11%</td>
</tr>
</tbody>
</table>

Table 5. The result of estimating the intrinsic error score using 3 seeds is within 16% of the estimation result using 9 seeds.

the intrinsic error score. Furthermore, we can tell which augmentations are effective versus those which are not effective from the three random seeds.

C. Supplementary Materials for Section 5

We describe details on our experiments to complement Section 5. In Appendix C.1, we review the datasets used in our experiments. In Appendix C.2, we describe the models we use on each dataset. In Appendix C.3, we summarize the training procedures for all experiments.

C.1. Datasets

We describe the image and text datasets used in the experiments in more detail.

Image datasets. For image classification tasks, the goal is to determine the object class shown in the image. We select four popular image classification benchmarks in our experiments.

MNIST. MNIST (LeCun et al., 1998) is a handwritten digit dataset with 60,000 training images and 10,000 testing images. Each image has size $28 \times 28$ and belongs to 1 of 10 digit classes.

CIFAR-10. CIFAR-10 (Krizhevsky et al., 2009) has 60,000 $32 \times 32$ color images in 10 classes, with 6,000 images per class where the training and test sets have 50,000 and 10,000 images, respectively.

CIFAR-100. CIFAR-100 is similar to CIFAR-10 while CIFAR-100 has 100 more fine-grained classes containing 600 images each.

Street view house numbers (SVHN). This dataset contains color house-number images with 73,257 core images for training and 26,032 digits for testing which is similar in flavor to MNIST.

ImageNet Large-Scale Visual Recognition Challenge (ImageNet). This dataset is a subset of original ImageNet dataset which has over 15M labeled high-resolution images belonging to roughly 22,000 categories. In this dataset, it includes images of 1000 classes, and has roughly 1.3M training images and 50,000 validation images.

Text dataset. For text classification task, the goal is to understand the sentiment opinions expressed in the text based on the context provided. We choose Internet movie database (IMDb).

Internet movie database (IMDb). IMDb (Maas et al., 2011) consists of a collection of 50,000 reviews, with no more than 30 reviews per movie. The dataset contains 25,000 labeled reviews for training and 25,000 for test.

C.2. Models

We describe the models we use in the our experiments.

Image datasets. For the experiments on image classification tasks, we consider five different models including multi-layer perceptron (MLP), Wide-ResNet, Shake-Shake (26 2x96d), PyramidNet+ShakeDrop, and ResNet.

For the MLP model, we reshape the image and feed it into a two layer perceptron, followed by a classification layer.

For the Wide-ResNet model, we use the standard Wide-ResNet model proposed by (Zagoruyko & Komodakis, 2016). We select two Wide-ResNet models in our experiment: Wide-ResNet-28-2 with depth 28 and width 2 as well as Wide-ResNet-28-10 with depth 28 and width 10.

For Shake-Shake, we use the model proposed by (Gastaldi, 2017) with depth 26, 2 residual branches. The first residual block has a width of 96, namely Shake-Shake (26 2x96d).
On the Generalization Effects of Linear Transformations in Data Augmentation

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Batch Size</th>
<th>LR</th>
<th>WD</th>
<th>LR Schedule</th>
<th>Epoch</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>MLP</td>
<td>500</td>
<td>0.1</td>
<td>0.0001</td>
<td>cosine</td>
<td>100</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>Wide-ResNet-28-2</td>
<td>128</td>
<td>0.1</td>
<td>0.0005</td>
<td>multi-step</td>
<td>200</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>Wide-ResNet-28-10</td>
<td>128</td>
<td>0.1</td>
<td>0.0005</td>
<td>cosine</td>
<td>200</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>Shake-Shake (26 2x96d)</td>
<td>128</td>
<td>0.01</td>
<td>0.001</td>
<td>cosine</td>
<td>1800</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>PyramidNet+ShakeDrop</td>
<td>64</td>
<td>0.05</td>
<td>0.00005</td>
<td>cosine</td>
<td>1800</td>
</tr>
<tr>
<td>CIFAR-100</td>
<td>Wide-ResNet-28-10</td>
<td>128</td>
<td>0.1</td>
<td>0.0005</td>
<td>cosine</td>
<td>200</td>
</tr>
<tr>
<td>SVHN</td>
<td>Wide-ResNet-28-10</td>
<td>128</td>
<td>0.005</td>
<td>0.005</td>
<td>cosine</td>
<td>200</td>
</tr>
<tr>
<td>ImageNet</td>
<td>ResNet-50</td>
<td>160</td>
<td>0.1</td>
<td>0.0001</td>
<td>multi-step</td>
<td>270</td>
</tr>
</tbody>
</table>

Table 6. Model hyperparameters on MNIST and CIFAR-10/CIFAR-100. LR means learning rate, WD means weight decay and LR Schedule means learning rate scheduling. The parameters we choose are based on the parameters used for the model previously.

For PyramidNet, we choose the model proposed by (Han et al., 2017) with ShakeDrop (Yamada et al., 2018). We set the depth as 272 and alpha as 200 in our experiments. We refer to the model as PyramidNet+ShakeDrop.

For ResNet, we select the model proposed by (He et al., 2016) with 50 layers. We refer to the model as ResNet-50.

For CIFAR-10 and CIFAR-100, after applying the transformations selected by Algorithm 1, we apply randomly cropping, horizontal flipping, cutout and mixup.

For ImageNet, we apply random resized cropping, horizontal flipping, color jitter and mixup after performing Algorithm 1. Similarly, for SVHN we apply randomly cropping and cutout after using Algorithm 1.

**Text dataset.** For the experiments on text classification tasks, we use a state-of-the-art language model call BERT (Devlin et al., 2018). We choose the BERT\textsubscript{LARGE} uncased model, which contains 24 layers of transformer.

### C.3. Training procedures.

We describe the training procedures for our experiments.

**Implementation details.** During the training process, for each image in a mini-batch during the optimization, we apply Algorithm 1 to find the most uncertain data points and use them to training the model. We only use the augmented data points to train the model and do not use the original data points. The specific transformations we use and the default transformations are already mentioned in Section 5.1.

**Image classification tasks.** We summarize the model hyperparameters for all the models in Table 6.

**Text classification tasks.** For text classification experiments, we follow the BERT\textsubscript{LARGE} fine-tune procedure proposed by (Devlin et al., 2018). We set the dropout rate of 0.1 and apply grid search to tune the learning rate from \{1e^{-5}, 2e^{-5}, 3e^{-5}\}, batch size of 32 and 64, and the number of epochs from 2 to 10.

### D. Additional Experiments on Mixup

We present additional experiments to provide micro insights on the effects of applying the mixup augmentation. First, we consider the performance of mixing same class images versus mixing different class images. We show that on CIFAR-10, mixup can reduce the intrinsic error score but mixing same class images does not reduce the intrinsic error score. Second, we consider the effect of mixup on the size of the margin of the classification model. We show that mixup corrects data points which have large margins from the baseline model.

**Training procedures.** We apply the MLP model on MNIST and the Wide-ResNet-28-10 model on CIFAR-10. For the training images, there is a default transformation of horizontal flipping with probability 0.5 and random cropping. Then we apply the mixup transformation.
Comparing mixup with $\ell_2$-regularization. We tune the optimal $\ell_2$ regularization parameter on the baseline model. Then, we run mixup with the optimal $\ell_2$ parameter. We also consider what happens if we only mix data points with the same class labels. Since mixup randomly mixes two images, the mixing ratio for same class images is 10%. Table 7 shows the results.

We make several observations. (i) Adding $\ell_2$ regularization reduces the instability score. This is expected since a higher value of $\lambda$ reduces the variance part in equation (1). (ii) On MNIST, mixing same class images improves stability compared to mixup. This is consistent with our results in Section 4. Furthermore, optimally tuning the regularization parameter outperforms mixup. (iii) on CIFAR-10, mixing same class images as well as mixup reduces the instability score by more than 10%. Furthermore, we observe that mixing different class images also reduces the intrinsic error score.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>MNIST</th>
<th>CIFAR-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>98.07%±0.08%</td>
<td>1.52%</td>
</tr>
<tr>
<td>Tuning $\ell_2$ reg.</td>
<td><strong>98.31%±0.05%</strong></td>
<td><strong>1.50%</strong></td>
</tr>
<tr>
<td>Mixup-same-class w/ $\ell_2$</td>
<td>98.15%±0.06%</td>
<td>1.78%</td>
</tr>
<tr>
<td>Mixup w/ $\ell_2$ reg.</td>
<td>98.21%±0.05%</td>
<td><strong>1.58%</strong></td>
</tr>
</tbody>
</table>

Table 7. Measuring the intrinsic error and instability scores of mixing same class images versus mixup. The optimal $\ell_2$ regularization parameter is $10^{-3}$ for MNIST and $5 \times 10^{-4}$ for CIFAR-10.

Effects over margin sizes on the cross-entropy loss. We further explore why mixup can improve the average prediction accuracy on CIFAR-10. Intuitively, when mixing two images with different losses, the resulting image will have a loss which is lower than the image with the higher loss. For the classification setting, instead of measuring the losses, we look at the margin, which is the difference between the largest predicted probability and the second largest predicted probability over the 10 classes. It is well-known that a larger margin implies better robustness and generalization properties (Friedman et al., 2001; Hastie et al., 2009).

By comparing the margin distribution between the baseline model versus the one after applying the mixup augmentations, we provide several interesting observations which shed more light on why mixup works. Figure 6 shows the results. First, we observe that among the images for which the baseline model predicts incorrectly, mixup is able to correct those images whose margin is very large! Second, we observe that among the images for which the baseline model predicts correctly, applying mixup increased the size of the margin for the images whose margin is small on the baseline model.

We further observe that the above effect arises from mixing different class images. We compare the effects of three settings, including i) Mix images from different classes only (Ratio 0.0). ii) For half of the time, mix images from different classes; Otherwise, mix images from the same classes (Ratio 0.5). iii) Mix images from the same classes only (Ratio 1.0). In Figure 6c, we observe the effect of correcting large margin data points does not occur when we only mix same class images.

Figure 6. On CIFAR-10, the images corrected by applying the mixup augmentation have large margins on the baseline model. Here the margin is defined as the largest probability minus the second largest probability predicted by the cross entropy loss. By varying the mixing ratio, we observe that mixing same class images only does not correct the the data points which are predicted incorrectly with large margins on the baseline model.