Affinity and Diversity: 
Quantifying Mechanisms of Data Augmentation

Raphael Gontijo-Lopes 1* Sylvia J. Smullin 2* Ekin D. Cubuk 1 Ethan Dyer 2

Abstract
Though data augmentation has become a standard component of deep neural network training, the underlying mechanism behind the effectiveness of these techniques remains poorly understood. In practice, augmentation policies are often chosen using heuristics of either distribution shift or augmentation diversity. Inspired by these, we seek to quantify how data augmentation improves model generalization. To this end, we introduce interpretable and easy-to-compute measures: Affinity and Diversity. We find that augmentation performance is predicted not by either of these alone but by jointly optimizing the two.

1. Introduction
Models that achieve state-of-the-art in image classification often use heavy data augmentation strategies. The best techniques use various transforms applied sequentially and stochastically. Though the effectiveness of such a technique is well-established, the mechanism through which these transformations work is not well-understood.

Since early uses of data augmentation in training neural networks, it has been assumed that they work because they simulate realistic samples from the true data distribution: “[augmentation strategies are] reasonable since the transformed reference data is now extremely close to the original data. In this way, the amount of training data is effectively increased” (Bellegarda et al., 1992). Because of this, augmentations have often been designed with the heuristic of incurring minimal distribution shift from the training data.

This rationale does not explain why unrealistic distortions such as cutout (DeVries & Taylor, 2017), SpecAugment (Park et al., 2019), and mixup (Zhang et al., 2017) significantly improve generalization performance. Furthermore, methods do not always transfer across datasets—

![Figure 1](image-url)

Figure 1. Affinity and Diversity parameterize the performance of a model trained with augmentation. (a) CIFAR-10: Color shows the final test accuracy. * marks the clean baseline. Each point represents a different augmentation that yields test accuracy greater than 88.7%. (b) Schematic representation of how clean data and augmented data are related to each other in the space of these two metrics. Higher data diversity is represented by a larger bubble while distributional similarity is depicted through the overlap between bubbles. Test accuracy generally improves to the upper right in this space. Adding real new data to the training set is expected to be in the far upper right corner.

Cutout, for example, is useful on CIFAR-10 and not on ImageNet (Lopes et al., 2019). Additionally, many augmentation policies heavily modify images by stochastically applying multiple transforms to a single image. Based on this observation, some have proposed that augmentation strategies are effective because they increase the diversity of images seen by the model.

In this complex landscape, claims about diversity and distributional similarity remain unverified heuristics. Without more precise data augmentation science, finding state-of-the-art strategies requires brute force that can cost thousands of GPU hours (Cubuk et al., 2018; Zhang et al., 2019). This highlights a need to specify and measure the relationship between the original training data and the augmented dataset, as relevant to a given model’s performance.

In this paper, we quantify these heuristics. Seeking to understand the mechanisms of augmentation, we focus on single transforms as a foundation. We present an extensive study—
of 204 different augmentations on CIFAR-10 and 223 on ImageNet, varying both broad transform families and finer transform parameters. Our contributions are:

1. We introduce Affinity and Diversity: interpretable, easy-to-compute metrics for parameterizing augmentation performance. Affinity quantifies how much an augmentation shifts the training data distribution from that learned by a model. Diversity quantifies the complexity of the augmented data with respect to the model and learning procedure.

2. We show that performance is dependent on both metrics. In the Affinity-Diversity plane, the best augmentation strategies jointly optimize the two (see Fig 1).

3. We connect augmentation to other familiar forms of regularization, such as $\ell_2$ and learning rate scheduling, observing common features of the dynamics: performance can be improved and training accelerated by turning off regularization at an appropriate time.

4. We show that performance is only improved when a transform increases the total number of unique training examples. The utility of these new training examples is informed by the augmentations Affinity and Diversity.

2. Related Work

Since early uses of data augmentation in training neural networks, there has been an assumption that effective transforms for data augmentation are those that produce images from an “overlapping but different” distribution (Bengio et al., 2011; Bellegarda et al., 1992). Indeed, elastic distortions as well as distortions in the scale, position, and orientation of training images have been used on MNIST (Ciregan et al., 2012; Sato et al., 2015; Simard et al., 2003; Wan et al., 2013), while horizontal flips, random crops, and random distortions to color channels have been used on CIFAR-10 and ImageNet (Krizhevsky et al., 2012; Zagoruyko & Komodakis, 2016; Zoph et al., 2017). For object detection and image segmentation, one can also use object-centric cropping (Liu et al., 2016) or cut-and-paste new objects (Dwibedi et al., 2017; Fang et al., 2019; Ngiam et al., 2019).

In contrast, researchers have also successfully used more generic transformations that are less domain-specific, such as Gaussian noise (Ford et al., 2019; Lopes et al., 2019), input dropout (Srivastava et al., 2014), erasing random patches of the training samples during training (DeVries & Taylor, 2017; Park et al., 2019; Zhong et al., 2017), and adversarial noise (Szegedy et al., 2013). Mixup (Zhang et al., 2017) and Sample Pairing (Inoue, 2018) are two augmentation methods that use convex combinations of training samples. It is also possible to further improve generalization by combining individual transformations. For example, reinforcement learning has been used to choose more optimal combinations of data augmentation transformations (Ratner et al., 2017; Cubuk et al., 2018). Follow-up research has lowered the computation cost of finding such optimal combinations, by either using population based training (Ho et al., 2019), density matching (Lim et al., 2019), adversarial policy-design that evolves throughout training (Zhang et al., 2019), or a reduced search space (Cubuk et al., 2019). Despite producing unrealistic outputs, such combinations of augmentations can be highly effective in different tasks (Berthelot et al., 2019; Tan & Le, 2019; Tan et al., 2019; Xie et al., 2019ab).

Across these different examples, the role of distribution shift in training remains unclear. Lim et al. (2019); Hataya et al. (2019) have found data augmentation policies by minimizing the distance between the distributions of augmented data and clean data. Recent work found that after training with augmented data, fine-tuning on clean training data for a few more epochs can be beneficial (He et al., 2019), while Touvron et al. (2019) found it beneficial to fine-tune with a test-set resolution that aligns with the training-set resolution.

The true input-space distribution from which a training dataset is drawn remains elusive. To better understand the effect of distribution shift on model performance, many works attempt to estimate it. Often these techniques require training secondary models, such as those based on variational methods (Goodfellow et al., 2014; Kingma & Welling, 2014; Nowozin et al., 2016; Blei et al., 2017). Others have tried to augment the training set by modelling the data distribution directly (Tran et al., 2017). Furthermore, recent work has suggested that even unrealistic distribution modelling can be beneficial (Dai et al., 2017).

These methods try to specify the distribution separately from the model they are trying to optimize. As a result, they are insensitive to any interaction between the model and data distribution. Instead, we are interested in a measure of how much the data shifts along directions that are most relevant to the model’s performance.

3. Methods

We performed extensive experiments with various augmentations on CIFAR-10 and ImageNet. Experiments on CIFAR-10 use the WRN-28-2 model (Zagoruyko & Komodakis, 2016), trained for 78k steps with cosine learning rate decay. Results given are the mean over 10 initializations and reported errors are the standard error on the mean. Errors are generally too small to show on figures. Details on the error analysis are in Sec. C.

Experiments on ImageNet use the ResNet-50 model (He
et al., 2016), trained for 112.6k steps with a weight decay rate of 1e-4, and a learning rate of 0.2, which is decayed by 10 at epochs 30, 60, and 80.

Images are pre-processed by dividing each pixel value by 255 and normalizing by the data set statistics. Random crop is also applied on all ImageNet models. When this pre-processed data is not further augmented, we refer to it as “clean data” and a model trained on it as the “clean baseline”. We follow the same implementation details as Cubuk et al. (2018), including for most augmentation operations. Further implementation details are in Sec. A.

For CIFAR-10, test accuracy on the clean baseline is 89.7 ± 0.1%. The validation accuracy is 89.9 ± 0.2%. On ImageNet, the test accuracy is 76.06%. Unless specified otherwise, data augmentation is applied following standard practice: each time an image is drawn, the given augmentation is applied with a given probability. We call this mode dynamic augmentation. Due to whatever stochasticity is in the transform itself (such as randomly selecting the location for a crop) or in the policy (such as applying a flip only with 50% probability), the augmented image could be different each time. Thus, most of the tested augmentations increase the number of possible distinct images that can be shown during training.

We also perform select experiments using static training. In static augmentation, the augmentation policy (one or more transforms) is applied once to the entire clean training set. Static augmentation does not change the number of unique images in the dataset.

3.1. Affinity: a simple metric for distribution shift

Thus far, heuristics of distribution shift have motivated design of augmentation policies. Inspired by this focus, we introduce a simple metric to quantify how augmentation shifts data with respect to the decision boundary of the clean baseline model.

We start by noting that a trained model is often sensitive to the distribution of the data it was trained on. That is, model performance varies greatly between new samples from the true data distribution and samples from a shifted distribution. Importantly, the distribution captured by the model is different from the input-space distribution, since training dynamics and the model’s implicit biases affect performance. Because the goal of data augmentation is improving model performance, measuring shifts with respect to this captured distribution is more meaningful than measuring shifts in the input-space distribution.

As such, we define Affinity to be the performance difference between the validation accuracy of a model trained on clean data, and the accuracy of the same model tested on an augmented validation set. Here, the augmentation is applied to the validation dataset in one pass, as a static augmentation. More formally we define:

**Definition 1.** Let \( D_{\text{train}} \) and \( D_{\text{val}} \) be training and validation datasets drawn IID from the same clean data distribution, and let \( D'_{\text{val}} \) be derived from \( D_{\text{val}} \) by applying a stochastic augmentation strategy, \( a \), once to each image in \( D_{\text{val}} \). \( D'_{\text{val}} = \{(a(x), y) : \forall (x, y) \in D_{\text{val}}\} \). Further let \( m \) be a model trained on \( D_{\text{train}} \) and \( \mathcal{A}(m, D) \) denote the model’s accuracy when evaluated on dataset \( D \). The Affinity, \( \mathcal{T}[a; m; D_{\text{val}}] \), is given by

\[
\mathcal{T}[a; m; D_{\text{val}}] = \mathcal{A}(m, D'_{\text{val}}) - \mathcal{A}(m, D_{\text{val}}).
\]

With this definition, Affinity of zero represents no shift and a negative number suggests that the augmented data is out-of-distribution for the model.

In Fig. 2 we illustrate Affinity with a two-class classification task on a mixture of two Gaussians. Augmentation in this example comprises shift of the means of the Gaussians of the validation data compared to those used for training. Under this shift, we calculate both Affinity and KL divergence of the shifted data with respect to the original data. Affinity changes only when the shift in the data is with respect to the model’s decision boundary, whereas the KL divergence changes even when data is shifted in the direction that is irrelevant to the classification task. In this way, Affinity captures what is relevant to a model: shifts that impact predictions.

This metric has appeared frequently as a measure of a model’s robustness. It has been used to measure robustness to corruptions of images that do not change their semantic
content (Azulay & Weiss, 2018; Dodge & Karam, 2017; Ford et al., 2019; Hendrycks & Dietterich, 2018; Rosenfeld et al., 2018; Yin et al., 2019). Here we, turn this around and use it to quantify the shift of augmented data compared to clean data.

Affinity has the following advantages as a metric:

1. It is easy to measure. It requires only clean training of the model in question.
2. It is independent of any confounding interaction between the data augmentation and the training process, since augmentation is only used on the validation set and applied statically.
3. It forms a measure of distance sensitive to properties of both the data distribution and the model.

We gain confidence in this metric by comparing it to other potential model-dependent measures of distribution shift. We consider the mean log likelihood of augmented test images (Grathwohl et al., 2019), and the Watanabe/Akaike information criterion (WAIC) (Watanabe, 2010). These other metrics have high correlation with Affinity. Details can be found in Sec. F.

3.2. Diversity: A measure of augmentation complexity

Inspired by the observation that multi-factor augmentation policies such as FlipLR+Crop+Cutout and RandAugment (Cubuk et al., 2019) greatly improve performance, we propose another axis on which to view augmentation policies, which we dub Diversity. This measure is intended to quantify the intuition that augmentations prevent models from over-fitting by increasing the number of samples in the training set; the importance of this is shown in Sec. 4.3.

Based on the intuition that more diverse data should be more difficult for a model to fit, we propose a model-based measure. The Diversity metric in this paper is the final training loss of a model trained with a given augmentation:

\[ \mathcal{D}_{\text{ent}} := H(X'|X) = -\mathbb{E}_{X} [\sum_{x} p(x'|X) \log(p(x'|X))] \]

Here \( x \in X \) is a clean training image and \( x' \in X' \) is an augmented image. This measure has the property that it can be evaluated without any training or reference to model architecture. However, calculating the entropy for continuously-varying transforms is less straightforward.

A third proxy for Diversity is the training time needed for a model to reach a given training accuracy threshold. In Sec. E, we show that these three Diversity metrics correlate well with each other, and that they all serve as complementary measure to Affinity for characterizing augmentation performance.

In the remaining sections we describe how the metrics of Diversity and Affinity can be used to understand augmentation performance.

4. Results

4.1. Augmentation performance is determined by both Affinity and Diversity

Despite the original inspiration to mimic realistic transformations and minimize distribution shift, many state-of-the-art augmentations yield unrealistic images. This suggests that distribution shift alone does not fully describe or predict augmentation performance.

Figure 3(a) (left) measures Affinity across 204 different augmentations for CIFAR-10 and 223 for ImageNet respectively. We find that for the most important augmentations—that those that help performance—Affinity is a poor predictor of accuracy. Furthermore, we find many successful augmentations with low Affinity. For example, Rotate(fixed, 45deg, 50%), Cutout(16), and combinations of FlipLR, Crop(32), and Cutout(16) all have Affinity< -15% and test accuracy> 2% above clean baseline on CIFAR-10. Augmentation details are in Sec. B.

As Affinity does not fully characterize the performance of an augmentation, we seek another metric. To assess the importance of an augmentation’s complexity, we measure Diversity across the same set of augmentations. We find that Diversity is complementary in explaining how augmentations can increase test performance. As shown in Fig. 3(b) and (c), Affinity and Diversity together provide a much
Figure 3. Augmentation performance is determined by both Affinity and Diversity. (a) Test accuracy plotted against each of Affinity and Diversity for the two datasets, showing that neither metric alone predicts performance. In the CIFAR-10 plots (top), blue highlights (also in inset) are the augmentations that increase test accuracy above the clean baseline. Dashed lines indicate the clean baseline. (b) and (c) show test accuracy on the color scale in the plane of Affinity and Diversity. The three star markers in (b) are (left to right) RandAugment, AutoAugment, and mixup. The * on the color bar indicates the clean baseline case. For fixed values of Affinity, test accuracy generally increases with higher values of Diversity. For fixed values of Diversity, test accuracy generally increases with higher values of Affinity.

A simple case study is presented in Fig. 4. The probability of the transform Rotate(fixed, 60deg) is varied. The accuracy and Affinity are not monotonically related, with the peak accuracy falling at an intermediate value of Affinity. Similarly, accuracy is correlated with Diversity for low probability transformations, but does not track for higher probabilities. The optimal probability for Rotate(fixed, 60deg) lies at an intermediate value of Affinity and Diversity.

To situate the tested augmentations—mostly single transforms—within the context of the state-of-the-art, we tested three high-performance augmentations from literature: mixup (Zhang et al., 2017), AutoAugment (Cubuk et al., 2018), and RandAugment (Cubuk et al., 2019). These are highlighted with a star marker in Fig. 3(b).

More than either of the metrics alone, Affinity and Diversity together provide a useful parameterization of an augmentation's performance. We now turn to investigating the utility of this tool for explaining other observed phenomena of data augmentations.

4.2. Turning augmentations off may adjust Affinity, Diversity, and performance

The term “regularizer” is ill-defined in the literature, often referring to any technique used to reduce generalization error without necessarily reducing training error (Goodfellow et al., 2016). With this definition, it is widely acknowledged that commonly-used augmentations act as regularizers (Hernández-García & König, 2018; Zhang et al., 2016; Dao et al., 2019). Though this is a broad definition, we notice another commonality across seemingly different kinds of regularizers: various regularization techniques yield boosts in performance (or at least no degradation) if the regularization is turned off at the right time during training. For instance:
To further study augmentation as a regularizer, we compare the constant augmentation case (with the same augmentation throughout) to the case where the augmentation is turned off partway through training and training is completed with clean data. For each transform, we test over a range of switch-off points and select the one that yields the best final validation or test accuracy on CIFAR-10 and ImageNet respectively. The Switch-off Lift is the resulting increase in final test accuracy, compared to training with augmented data the entire time.

For some poor-performing augmentations, this gain can actually bring the final test accuracy above the baseline, as shown in Fig. 5(b). We additionally observe (Fig. 5(a)) that this test accuracy improvement can happen quite rapidly for both augmentations and for the other regularizers tested. This suggests an opportunity to accelerate training without hurting performance by appropriately switching off regularization. We call this a “slingshot” effect.

Interestingly, the best time for turning off an augmentation is not always close to the end of training, contrary to what is shown in He et al. (2019). For example, without switching, FlipUD(100%) decreases test accuracy by almost 50% compared to clean baseline. When the augmentation is used for only the first third of training, final test accuracy is above the baseline.

**Figure 5.** (a) **Switching off regularizers yields performance boost.** Three examples of how turning off a regularizer creates a fast increase in validation accuracy as a function of the training step. This slingshot effect can speed up training and improve the best validation accuracy. Top: training with no augmentation (clean baseline), compared to constant augmentation, and augmentation that is turned off at 55k steps. Here, the augmentation is Rotate(fixed, 20deg, 100%). Middle: Baseline with constant \(\ell_2\). This is compared to turning off \(\ell_2\) regularization part way through training. Bottom: Constant learning rate of 0.1 compared to training where the learning rate is decayed in one step by a factor of 10. (b) **Bad augmentations can become helpful if switched off:** Colored lines connect the test accuracy with augmentation applied throughout training (top) to the test accuracy with switching mid-training. Color indicates the amount of Switch-off Lift; blue is positive and orange is negative.

1. Decaying a large learning rate on an appropriate schedule can be better than maintaining a large learning rate throughout training (Zagoruyko & Komodakis, 2016).

2. Turning off \(\ell_2\) regularization at the right time in training does not hurt performance (Golatkar et al., 2019).

3. Relaxing architectural constraints mid-training can boost final performance (d’Ascoli et al., 2019).

4. Turning augmentations off and fine-tuning on clean data can improve final test accuracy (He et al., 2019).

**Figure 6.** Switch-off Lift varies with Affinity and Diversity. Where Switch-off Lift is negative, it is mapped to 0 on the color scale.

He et al. (2019) hypothesized that the gain from turning augmentation off is due to recovery from the augmentation distribution shift. Indeed, for many detrimental transformations, the test accuracy gained by turning off the augmentation merely recovers the clean baseline performance. However, in Fig. 6, we see that for a given value of Affinity, Switch-off Lift can vary. This is most clear for more useful augmentations, suggesting that the Switch-off Lift is derived from more than simply correction of a distribution shift.

A few of the tested augmentations, such as FlipLR(100%), are fully deterministic. Thus, each time an image is drawn in training, it is augmented the same way. When such an
augmentation is turned off partway through training, the model then sees images—the clean ones—that are now new. Indeed, when FlipLR(100%) is switched off at the right time, its final test accuracy exceeds that of FlipLR(50%) without switching. In this way, switching augmentation off may adjust for not only low Affinity but also low Diversity.

4.3. Increased effective training set size is crucial for data augmentation

Figure 7. Static augmentations never improve performance. On CIFAR-10, static augmentation performance on tested augmentations is less than the clean baseline, (0, 0), and less than the dynamic augmentation case. Diagonal line indicates where static augmentation would equal dynamic augmentation. Augmentations with no stochasticity are excluded because they are trivially equal on the two axes.

Most of the augmentations we tested and those used in practice have inherent stochasticity and thus may alter a given training image differently each time the image is drawn. In the typical dynamic training mode, these augmentations increase the number of unique inputs seen across training epochs.

To further study how augmentations act as regularizers, we seek to discriminate this increase in effective dataset size from other effects. We train models with static augmentation, as described in Sec. 3. This altered training set is used without further modification during training so that the number of unique training inputs is the same between the augmented and the clean training settings.

For almost all tested augmentations, using static augmentation yields lower test accuracy than the clean baseline. In the tested cases where static augmentation shows a gain (versions of crop), the difference is less than the standard error on the mean. Additionally, the decrease in performance for static augmentation, compared to the clean baseline, is greater for transforms that have lower Affinity and lower Diversity. Finally, static augmentations always perform worse than their non-deterministic, dynamic counterparts. As shown in Fig. 7, these results point to the following conclusion:

Increased effective training set size is crucial to the performance benefit of data augmentation. An augmentation’s Affinity and Diversity inform how useful the additional training examples are.

5. Discussion

In this work, we focused on single transforms in an attempt to understand the essential parts of augmentation in a controlled context. This builds a foundation for further exploration, including using these metrics to quantify and design more complex and powerful combinations of augmentations.

Though earlier work has often explicitly focused on just one of these metrics, the priors used have implicitly ensured reasonable values for both. One way to achieve Diversity is to use combinations of many single augmentations, as exemplified in Cubuk et al. (2018). Because the transforms and hyperparameters in Cubuk et al. (2018) were chosen by optimizing performance on proxy tasks, the optimal policies do include high Affinity and low Affinity transforms. Fast AutoAugment (Lim et al., 2019), CTAugment (Berthelot et al., 2019; Sohn et al., 2020), and differentiable RandAugment (Cubuk et al., 2019) all aim to increase Affinity by what Lim et al. (2019) called “density-matching”. However these methods all use the search space of AutoAugment and inherit its Diversity.

On the other hand, Adversarial AutoAugment (Zhang et al., 2019) focused on increasing Diversity by optimizing policies to increase the training loss. While this method did not explicitly aim to increase Affinity, it also used transforms and hyperparameters from the AutoAugment search space. Without such a prior, which includes useful Affinity, the goal of maximizing training loss with no other constraints would lead to data augmentation policies that erase all the information from the images.

Our results motivate casting an even wider net when searching for augmentation strategies. Firstly, our work suggests that explicitly optimizing along axes of both Affinity and Diversity yields better performance. Furthermore, we have seen that poor-performing augmentations can actually be helpful if turned off during training (Figure 5). With inclusion of scheduling in augmentation optimization, we expect there are opportunities for including a different set of augmentations in an ideal policy. Ho et al. (2019) observes trends in how probability and magnitude of various trans-
forms change during training for an optimized augmentation schedule. We suggest that with further study, Diversity and Affinity can provide priors for optimization of augmentation schedules.

6. Conclusion

We attempted to quantify common intuition that more in-distribution and more diverse augmentation policies perform well. To this end, we introduced two easy-to-compute metrics, Affinity and Diversity, intended to measure to what extent a given augmentation is in-distribution and how complex the augmentation is to learn. Because they are model-dependent, these metrics capture the data shifts that affect model performance.

Using these tools, we have conducted a study over a large class of augmentations for CIFAR-10 and ImageNet and found that neither feature alone is a perfect predictor of performance. Rather, we presented evidence that an augmentation’s Diversity and Affinity play dual roles in determining augmentation quality. Optimizing for either metric separately is sub-optimal and the best augmentations balance the two.

Additionally, we found that increased sample number was a necessary ingredient of beneficial augmentation.

Finally, we found that augmentations share an important feature with other regularizers: switching off regularization at the right time can improve performance. In some cases, this can cause an otherwise poorly-performing augmentation to be beneficial.

We hope our findings provide a foundation and context for continued scientific study of data augmentation.

Acknowledgments

The authors would like to thank Alex Alemi, Justin Gilmer, Guy Gur-Ari, Albin Jones, Behnam Neyshabur, and Ben Poole for thoughtful discussions on this work.

References

Azulay, A. and Weiss, Y. Why do deep convolutional networks generalize so poorly to small image transformations? arXiv preprint arXiv:1805.12177, 2018.

Bellegarda, J. R., de Souza, P. V., Nadas, A. J., Nahamoo, D., Picheny, M. A., and Bahl, L. R. Robust speaker adaptation using a piecewise linear acoustic mapping. In ICASSP-92: 1992 IEEE International Conference on Acoustics, Speech, and Signal Processing, 1992.

Bengio, Y., Bastien, F., Bergeron, A., Boulanger-Lewandowski, N., Breuel, T., Chherawala, Y., Cisse, M., Côté, M., Erhan, D., Eustache, J., et al. Deep learners benefit more from out-of-distribution examples. In Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, pp. 164–172, 2011.

Berthelot, D., Carlini, N., Cubuk, E. D., Kurakin, A., Sohn, K., Zhang, H., and Raffel, C. Remixmatch: Semi-supervised learning with distribution alignment and augmentation anchoring. arXiv preprint arXiv:1911.09785, 2019.

Blei, D. M., Kucukelbir, A., and McAuliffe, J. D. Variational inference: A review for statisticians. Journal of the American Statistical Association, 112(518):859877, Feb 2017. ISSN 1537-274X. doi: 10.1080/01621459.2017.1285773. URL http://dx.doi.org/10.1080/01621459.2017.1285773.

Ciregan, D., Meier, U., and Schmidhuber, J. Multi-column deep neural networks for image classification. In Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, pp. 3642–3649. IEEE, 2012.

Cubuk, E. D., Zoph, B., Mane, D., Vasudevan, V., and Le, Q. V. Autoaugment: Learning augmentation policies from data. arXiv preprint arXiv:1805.09501, 2018.

Cubuk, E. D., Zoph, B., Shlens, J., and Le, Q. V. Randaugment: Practical data augmentation with no separate search. arXiv preprint arXiv:1909.13719, 2019.

Dai, Z., Yang, Z., Yang, F., Cohen, W. W., and Salakhutdinov, R. R. Good semi-supervised learning that requires a bad gan. In Advances in neural information processing systems, pp. 6510–6520, 2017.

Dao, T., Gu, A., Ratner, A. J., Smith, V., De Sa, C., and Ré, C. A kernel theory of modern data augmentation. Proceedings of machine learning research, 97:1528, 2019.

d’Ascoli, S., Sagun, L., Bruna, J., and Birolì, G. Finding the needle in the haystack with convolutions: on the benefits of architectural bias, 2019.

DeVries, T. and Taylor, G. W. Improved regularization of convolutional neural networks with cutout. arXiv preprint arXiv:1708.04552, 2017.

Dodge, S. and Karam, L. A study and comparison of human and deep learning recognition performance under visual distortions. In 2017 26th international conference on computer communication and networks (ICCCN), pp. 1–7. IEEE, 2017.

Dwibedi, D., Misra, I., and Hebert, M. Cut, paste and learn: Surprisingly easy synthesis for instance detection. In Proceedings of the IEEE International Conference on Computer Vision, pp. 1301–1310, 2017.
Fang, H.-S., Sun, J., Wang, R., Gou, M., Li, Y.-L., and Lu, C. Instaboost: Boosting instance segmentation via probability map guided copy-pasting. In Proceedings of the IEEE International Conference on Computer Vision, pp. 682–691, 2019.

Ford, N., Gilmer, J., Carlini, N., and Cubuk, D. Adversarial examples are a natural consequence of test error in noise. arXiv preprint arXiv:1901.10513, 2019.

Golatkar, A., Achille, A., and Soatto, S. Time matters in regularizing deep networks: Weight decay and data augmentation affect early learning dynamics, matter little near convergence, 2019.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. Generative adversarial nets. In Ghahramani, Z., Welling, M., Cortes, C., Lawrence, N. D., and Weinberger, K. Q. (eds.), Advances in Neural Information Processing Systems 27, pp. 2672–2680. Curran Associates, Inc., 2014. URL http://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf.

Grathwohl, W., Wang, K.-C., Jacobsen, J.-H., Duvenaud, D., Norouzi, M., and Swersky, K. Your classifier is secretly an energy based model and you should treat it like one, 2019.

Hataya, R., Zdenek, J., Yoshizoe, K., and Nakayama, H. Faster autoaugment: Learning augmentation strategies using backpropagation, 2019.

He, K., Zhang, X., Ren, S., and Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016.

Hendrycks, D. and Dietterich, T. G. Benchmarking neural network robustness to common corruptions and surface variations. arXiv preprint arXiv:1807.01697, 2018.

Hernández-García, A. and König, P. Further advantages of data augmentation on convolutional neural networks. In International Conference on Artificial Neural Networks, pp. 95–103. Springer, 2018.

Ho, D., Liang, E., Stoica, I., Abbeel, P., and Chen, X. Population based augmentation: Efficient learning of augmentation policy schedules. arXiv preprint arXiv:1905.05393, 2019.

Inoue, H. Data augmentation by pairing samples for images classification. arXiv preprint arXiv:1801.02929, 2018.

Kingma, D. P. and Welling, M. Auto-encoding variational bayes. In Bengio, Y. and LeCun, Y. (eds.), ICLR, 2014. URL http://dblp.uni-trier.de/db/conf/iclr/iclr2014.html#KingmaW13.

Krizhevsky, A., Sutskever, I., and Hinton, G. E. Imagenet classification with deep convolutional neural networks. In Advances in Neural Information Processing Systems, 2012.

Lim, S., Kim, I., Kim, T., Kim, C., and Kim, S. Fast autoaugment. arXiv preprint arXiv:1905.00397, 2019.

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., and Berg, A. C. Ssd: Single shot multibox detector. In European conference on computer vision, pp. 21–37. Springer, 2016.

Lopes, R. G., Yin, D., Poole, B., Gilmer, J., and Cubuk, E. D. Improving robustness without sacrificing accuracy with patch gaussian augmentation. arXiv preprint arXiv:1906.02611, 2019.

Ngiam, J., Caine, B., Han, W., Yang, B., Chai, Y., Sun, P., Zhou, Y., Yi, X., Alsharif, O., Nguyen, P., et al. Starnet: Targeted computation for object detection in point clouds. arXiv preprint arXiv:1908.11069, 2019.

Nowozin, S., Cseke, B., and Tomioka, R. f-gan: Training generative neural samplers using variational divergence minimization, 2016.

Park, D. S., Chan, W., Zhang, Y., Chiu, C.-C., Zoph, B., Cubuk, E. D., and Le, Q. V. Specaugment: A simple data augmentation method for automatic speech recognition. arXiv preprint arXiv:1904.08779, 2019.

Ratner, A. J., Ehrenberg, H., Hussain, Z., Dunnmon, J., and Ré, C. Learning to compose domain-specific transformations for data augmentation. In Advances in Neural Information Processing Systems, pp. 3239–3249, 2017.

Rosenfeld, A., Zemel, R., and Tsotsos, J. K. The elephant in the room. arXiv preprint arXiv:1808.03305, 2018.

Sato, I., Nishimura, H., and Yokoi, K. Apac: Augmented pattern classification with neural networks. arXiv preprint arXiv:1505.03229, 2015.

Simard, P. Y., Steinkraus, D., Platt, J. C., et al. Best practices for convolutional neural networks applied to visual document analysis. In Proceedings of International Conference on Document Analysis and Recognition, 2003.
Sohn, K., Berthelot, D., Li, C.-L., Zhang, Z., Carlini, N., Cubuk, E. D., Kurakin, A., Zhang, H., and Raffel, C. Fixmatch: Simplifying semi-supervised learning with consistency and confidence. *arXiv preprint arXiv:2001.07685*, 2020.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1):1929–1958, 2014.

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., and Fergus, R. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013.

Tan, M. and Le, Q. V. Efficientnet: Rethinking model scaling for convolutional neural networks. *arXiv preprint arXiv:1905.11946*, 2019.

Tan, M., Pang, R., and Le, Q. V. Efficientdet: Scalable and efficient object detection. *arXiv preprint arXiv:1911.09070*, 2019.

Touvron, H., Vedaldi, A., Douze, M., and Jgou, H. Fixing the train-test resolution discrepancy, 2019.

Tran, T., Pham, T., Carneiro, G., Palmer, L., and Reid, I. A bayesian data augmentation approach for learning deep models. In *Advances in Neural Information Processing Systems*, pp. 2794–2803, 2017.

Wan, L., Zeiler, M., Zhang, S., Le Cun, Y., and Fergus, R. Regularization of neural networks using dropconnect. In *International Conference on Machine Learning*, pp. 1058–1066, 2013.

Watanabe, S. Asymptotic equivalence of bayes cross validation and widely applicable information criterion in singular learning theory. *J. Mach. Learn. Res.*, 11:35713594, December 2010. ISSN 1532-4435.

Xie, C., Tan, M., Gong, B., Wang, J., Yuille, A., and Le, Q. V. Adversarial examples improve image recognition. *arXiv preprint arXiv:1911.09665*, 2019a.

Xie, Q., Dai, Z., Hovy, E., Luong, M.-T., and Le, Q. V. Unsupervised data augmentation. *arXiv preprint arXiv:1904.12848*, 2019b.

Zoph, B., Vasudevan, V., Shlens, J., and Le, Q. V. Learning transferable architectures for scalable image recognition. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, 2017.
Affinity and Diversity:
Quantifying Mechanisms of Data Augmentation
Supplement

A. Training methods
Cifar10 models are trained using code that is based on AutoAugment code\(^2\) using the following choices:

1. Learning rate is decayed following a cosine decay schedule, starting with a value of 0.1
2. 78050 training steps, with data shuffled after every epoch.
3. As implemented in the AutoAugment code, model is WRN-28-2 with stochastic gradient descent and momentum. Optimizer uses cross entropy loss with \(\ell_2\) weight decay of 0.0005.
4. Before selecting the validation set, the full training set is shuffled and balanced such that the subset selected for training is balanced across classes.
5. Validation set is the last 5000 samples of the shuffled CIFAR-10 training data.
6. Models trained using Python 2.7 and TensorFlow 1.13.

A training time of 78k steps was chosen because it shows reasonable convergence with the standard data augmentation of FlipLR, Crop, and Cutout. In the clean baseline case, test accuracy actually reaches its peak much earlier than 78k steps.

With CIFAR-10, experiments were also performed for dataset sizes of 1024, 4096, and 16384. At smaller dataset sizes, the impact of augmentation and the Switch-off Lift tends to be larger. These results are not shown in this paper.

ImageNet models are ResNet-50 trained using the Cloud TPU codebase\(^3\). Models are trained for 112.6k steps with a weight decay rate of 1e-4, and a learning rate of 0.2, which is decayed by 10 at epochs 30, 60, and 80. Batch size was set to be 1024.

B. Details of augmentation
B.1. CIFAR-10
On CIFAR-10, both color and affine transforms were tested, as given in the full results (see Sec. G). Most augmentations are as defined in Cubuk et al. (2018). For Rotate, fixed means each augmented image is rotated by exactly the stated amount, with randomly-chosen direction. Variable means an augmented image is rotated a random amount up to the given value. Shear is defined similarly. Rotate(square) means that an image is rotated by an amount chosen randomly from \([0^\circ, 90^\circ, 180^\circ, 270^\circ]\).

Crop includes a padding before the random-location crop so that the final image remains 32 x 32 in size. The magnitude given for Crop is the number of pixels that are added in each dimension. The magnitude given in Cutout is the size, in pixels, of each dimension of the square cutout.

PatchGaussian is as defined in Lopes et al. (2019), with the patch specified to be contained entirely within the image domain. It is specified by two hyperparameters: the size of the square patch (in pixels) and \(\sigma_{\text{max}}\), which is the maximum standard deviation of the noise that can be selected for any given patch. Here, “fixed” means the patch size is always the same.

\(^2\)available at github.com/tensorflow/models/tree/master/research/autoaugment
\(^3\)available at https://github.com/tensorflow/tpu/tree/master/models/official/resnet
Since FlipLR, Crop, and Cutout are part of standard pipelines for CIFAR-10, we test combinations of the three augmentations (varying probabilities of each) as well as these three augmentations plus an single additional augmentation. As in standard processing of CIFAR-10 images, the first augmentation applied is anything that is not one of FlipLR, Crop, or Cutout. After that, augmentations are applied in the order Crop, then FlipLR, then Cutout.

Finally, we tested the CIFAR-10 AutoAugment policy (Cubuk et al., 2018), RandAugment (Cubuk et al., 2019), and mixup (Zhang et al., 2017). The hyperparameters for these augmentations followed the guidelines described in the respective papers.

These augmentations are labeled in Fig. 8.

### B.2. ImageNet

On ImageNet, we experimented with PatchGaussian, Cutout, operations from the PIL imaging library[^4], and techniques from the AutoAugment code, as described above for CIFAR-10. In addition to PatchGaussian(fixed), we also tested PatchGaussian(variable), where the patch size is uniformly sampled up to a maximum size. The implementation here does not constrain the patch to be entirely contained within the image. Additionally, we experimented with SolarizeAdd. SolarizeAdd is similar to Solarize from the PIL library, but has an additional hyperparameter which determines how much value is added to each pixel that is below the threshold. Finally, we also experimented with Full Gaussian and Random Erasing on ImageNet. Full Gaussian adds Gaussian noise to the whole image. Random Erasing is similar to Cutout, but randomly samples the values of the pixels in the patch (Zhong et al., 2017) (whereas Cutout sets them to a constant, gray pixel).

These augmentations are labeled in Fig. 9.

Each augmentation is applied with a certain probability (given as a percentage in the label). Each time an image is pulled for training, the given image is augmented with that probability.

### C. Error analysis

All of the CIFAR-10 experiments were repeated with 10 different initialization. In most cases, the standard error on the mean (SEM) is too small to show as error bars on plots. The error on each measurement is given in the full results (see Sec. G).

Affinity and Switch-off Lift both are computed from differences between runs that share the same initialization. For Affinity, the same trained model is used for inference on clean validation data and on augmented validation data. Thus, the variance of Affinity for the clean baseline is not independent of the variance of Affinity for a given augmentation. The difference between the augmentation case and the clean baseline case is taken on a per-experiment basis (for each initialization of the clean baseline model) before the error is computed.

In the switching experiments, the final training without augmentation is computed starting from a given checkpoint in the model that is trained with augmentation. Thus, each switching experiment shares an initialization with an experiment that has no switching. Again, in this case the difference is taken on a per-experiment basis before the error (based on the standard deviation) is computed.

All ImageNet experiments shown are with one initialization. Thus, there are not statistics from which to analyze the error.

### D. Switching off augmentations

For CIFAR-10, switching times are tested in increments of approximately 5k steps between ~ 25k and ~ 75k steps. The best point for switching is determined by the final validation accuracy.

On ImageNet, we tested turning augmentation off at 50, 60, 70, and 80 epochs. Total training takes 90 epochs. The best point for switching is determined by the final test accuracy.

The Switch-off Lift is derived from the experiment at the best switch-off point for each augmentation.

There are some augmentations where the validation accuracy is best at 25k, which means that further testing is needed to

[^4]: https://pillow.readthedocs.io/en/5.1.x/
find if the actual optimum switch off point is lower or if the best case is to not train at all with the given augmentation. Some of the best augmentations have a small negative Switch-off Lift, indicating that it is better to train the entire time with the given augmentations.

For each augmentation, the best time for switch-off is listed in the full results (see Sec. G).

E. Diversity metrics

We compute three possible diversity metrics, shown in Fig. 10: Entropy, Final Training Loss, Training Steps to Accuracy Threshold. The entropy is calculated only for augmentations that have a discrete stochasticity (such as Rotate(fixed)) and not for augmentations that have a continuous variation (such as Rotate(variable) or PatchGaussian). Final Training Loss is the batch statistic at the last step of training. For CIFAR-10 experiments, this is averaged across the 10 initializations. For ImageNet, it is averaged over the last 10 steps of training. Training Steps to Accuracy Threshold is the number of training steps at which the training accuracy first hits a threshold of 97%. A few of the tested augmentation (extreme versions of PatchGaussian) do not reach this threshold in the given time and that column is left blank in the full results.

Entropy is unique in that it is independent of the model or data set and it is a counting of states. However, it is difficult to compare between discrete and continuously-varying transforms and it is not clear how proper it is to compare even across different types of transforms.

Final Training Loss and Training Steps to Accuracy Threshold correlate well across the tested transforms. Entropy is highly correlated to these measures for PatchGaussian and versions of FlipLR, Crop, and Cutout where only probabilities are varying. For Rotate and Shear where magnitudes are varying as well, the correlation between Entropy and the other two measures is less clear.

F. Comparing Affinity to other related measures

We gain confidence in the Affinity measure by comparing it to other potential model-dependant measures of distribution shift. In Fig 11, we show the correlation between Affinity and these two measures: the mean log likelihood of augmented test images(Grathwohl et al., 2019) (labeled as “logsumexp(logits)”) and the Watanabe Akaike information criterion (labeled as “WAIC”) (Watanabe, 2010).

Like Affinity, these other two measures indicate how well a model trained on clean data comprehends augmented data.

G. Full results

The plotted data for CIFAR-10 and ImageNet are given in .csv files uploaded at https://storage.googleapis.com/public_research_data/augmentation/data.zip. In these .csv files, blank cells generally indicate that a given experiment (such as switching) was not done for the specified augmentation. In the case of the training accuracy threshold as a proxy for diversity, a blank cell indicates that for the given augmentation, the training accuracy did not reach the specified threshold during training.
Figure 8. CIFAR-10: Labeled map of tested augmentations on the plane of Affinity and Diversity. Color distinguishes different hyperparameters for a given transform. Legend is below.
Diversity  

**Affinity**

- Clean
- Autoaugment
- Mixup
- Randaug
- PatchGaussian(fixed, 8, 2.0, 100%)
- PatchGaussian(fixed, 8, 1.5, 100%)
- PatchGaussian(fixed, 8, 1.0, 100%)
- PatchGaussian(fixed, 8, 0.8, 100%)
- PatchGaussian(fixed, 8, 0.5, 100%)
- PatchGaussian(fixed, 8, 0.3, 100%)
- PatchGaussian(fixed, 8, 0.2, 100%)
- PatchGaussian(fixed, 8, 0.1, 100%)
- PatchGaussian(fixed, 4, 2.0, 100%)
- PatchGaussian(fixed, 4, 1.5, 100%)
- PatchGaussian(fixed, 4, 1.0, 100%)
- PatchGaussian(fixed, 4, 0.8, 100%)
- PatchGaussian(fixed, 4, 0.5, 100%)
- PatchGaussian(fixed, 4, 0.3, 100%)
- PatchGaussian(fixed, 4, 0.1, 100%)
- PatchGaussian(fixed, 32, 2.0, 100%)
- PatchGaussian(fixed, 28, 2.0, 100%)
- PatchGaussian(fixed, 28, 1.5, 100%)
- PatchGaussian(fixed, 28, 1.0, 100%)
- PatchGaussian(fixed, 28, 0.8, 100%)
- PatchGaussian(fixed, 28, 0.5, 100%)
- PatchGaussian(fixed, 28, 0.3, 100%)
- PatchGaussian(fixed, 28, 0.2, 100%)
- PatchGaussian(fixed, 28, 0.1, 100%)
- PatchGaussian(fixed, 24, 2.0, 100%)
- PatchGaussian(fixed, 24, 1.5, 100%)
- PatchGaussian(fixed, 24, 1.0, 100%)
- PatchGaussian(fixed, 24, 0.8, 100%)
- PatchGaussian(fixed, 24, 0.5, 100%)
- PatchGaussian(fixed, 24, 0.3, 100%)
- PatchGaussian(fixed, 24, 0.2, 100%)
- PatchGaussian(fixed, 24, 0.1, 100%)
- PatchGaussian(fixed, 20, 2.0, 100%)
- PatchGaussian(fixed, 20, 1.5, 100%)
- PatchGaussian(fixed, 20, 1.0, 100%)
- PatchGaussian(fixed, 20, 0.8, 100%)
- PatchGaussian(fixed, 20, 0.5, 100%)
- PatchGaussian(fixed, 20, 0.3, 100%)
- PatchGaussian(fixed, 20, 0.2, 100%)
- PatchGaussian(fixed, 20, 0.1, 100%)
- PatchGaussian(fixed, 16, 2.0, 100%)
- PatchGaussian(fixed, 16, 1.5, 100%)
- PatchGaussian(fixed, 16, 1.0, 100%)
- PatchGaussian(fixed, 16, 0.8, 100%)
- PatchGaussian(fixed, 16, 0.5, 100%)
- PatchGaussian(fixed, 16, 0.3, 100%)
- PatchGaussian(fixed, 16, 0.2, 100%)
- PatchGaussian(fixed, 16, 0.1, 100%)

**Randaug**

- FlipLR(50%)
- Mixup
- Autoaugment
- Clean
- Equalize(50%) + Cutout(16, 100%)
- Equalize(50%) + Cutout(16, 75%)
- Equalize(50%) + Cutout(16, 25%)
- Cutout(16, 100%)
- Cutout(16, 75%)
- Cutout(16, 25%)

**Mixup**

- FlipLR(50%)
- Mixup
- Autoaugment
- Clean
- Equalize(50%) + Cutout(16, 100%)
- Equalize(50%) + Cutout(16, 75%)
- Equalize(50%) + Cutout(16, 25%)
- Cutout(16, 100%)
- Cutout(16, 75%)
- Cutout(16, 25%)

**Autoaugment**

- FlipLR(50%)
- Mixup
- Autoaugment
- Clean
- Equalize(50%) + Cutout(16, 100%)
- Equalize(50%) + Cutout(16, 75%)
- Equalize(50%) + Cutout(16, 25%)
- Cutout(16, 100%)
- Cutout(16, 75%)
- Cutout(16, 25%)

**Clean**

- FlipLR(50%)
- Mixup
- Autoaugment
- Clean
- Equalize(50%) + Cutout(16, 100%)
- Equalize(50%) + Cutout(16, 75%)
- Equalize(50%) + Cutout(16, 25%)
- Cutout(16, 100%)
- Cutout(16, 75%)
- Cutout(16, 25%)
Figure 9. ImageNet: Labeled map of tested augmentations on the plane of Affinity and Diversity. Color distinguishes different hyperparameters for a given transform. Legend is below.
| Diversity | Typicality |
|-----------|------------|
| Clean     |            |
| Patch Gaussian (variable, 100, 0.2, 100%) |            |
| Patch Gaussian (variable, 100, 0.5, 100%) |            |
| Patch Gaussian (variable, 100, 0.8, 100%) |            |
| Patch Gaussian (variable, 100, 1.0, 100%) |            |
| Patch Gaussian (variable, 100, 2.0, 100%) |            |
| Patch Gaussian (variable, 150, 0.2, 100%) |            |
| Patch Gaussian (variable, 150, 0.5, 100%) |            |
| Patch Gaussian (variable, 150, 0.8, 100%) |            |
| Patch Gaussian (variable, 150, 1.0, 100%) |            |
| Patch Gaussian (variable, 150, 2.0, 100%) |            |
| Typicality |            |
| 1.5        |            |
| 2.0        |            |
| 2.5        |            |
| 3.0        |            |
| 3.5        |            |

Affinity and Diversity: Quantifying Mechanisms of Data Augmentation
Figure 10. CIFAR-10: Three different diversity metrics are strongly correlated for high entropy augmentations. Here, the entropy is calculated only for discrete augmentations.

Figure 11. Affinity correlates with two other measures of how augmented images are related to a trained model’s distribution: \( \log \text{sumexp} \) of the logits (left, for CIFAR-10, and right, for ImageNet) is the mean log likelihood for the image. WAIC (middle, for CIFAR-10) corrects for a possible bias in that estimate. All these plots, numbers are referenced to the clean baseline, which is assigned a value of 0.