Augmentation Inside the Network

Maciej Sypetkowski
Faculty of Mathematics, Informatics and Mechanics
University of Warsaw
Email: m.sypetkowski@student.uw.edu.pl

Jakub Jasiulewicz
Faculty of Mathematics, Informatics and Mechanics
University of Warsaw
Email: j.jasiulewicz@student.uw.edu.pl

Zbigniew Wojna
University College London
Tensorflight Inc.
Email: zbigniewwojna@gmail.com

Abstract—In this paper, we present augmentation inside the network, a method that simulates data augmentation techniques for computer vision problems on intermediate features of a convolutional neural network. We perform these transformations, changing the data flow through the network, and sharing common computations when it is possible. Our method allows us to obtain smoother speed-accuracy trade-off adjustment and achieves better results than using standard test-time augmentation (TTA) techniques. Additionally, our approach can improve model performance even further when coupled with test-time augmentation. We validate our method on the ImageNet-2012 and CIFAR-100 datasets for image classification. We propose a modification that is 30% faster than the flip test-time augmentation and achieves the same results for CIFAR-100.

I. INTRODUCTION

Since the first successful uses of deep convolutional networks for the task of image classification [1], [2], these architectures have dominated the field, and their various iterations are to this day regarded as state of the art.

Much work and focus of researchers have been put into innovating and improving on previous network architectures [3], [4], [5], [6], [7], [8], [9].

Some problems can be tackled in the architecture, in particular, convolutional neural networks were designed to be unaffected by translations, and Harmonic Networks [10] are an architecture which is locally equivariant to patch-wise translation and rotation.

One other improvement is the use of data augmentation, which is standard in modern approaches to image classification, yet has seen much slower improvement over techniques used already in 2012 [2].

State of the art computer vision techniques take advantage of test-time augmentation when aiming for the highest possible score [11], [12], at the cost of additional computation time during inference. Our goal in this work is to simulate TTA as part of the neural architecture.

Traditional data augmentation techniques based on performing separate calculations on multiple transformed copies of the input image can be regarded as branching the network out at the very start, performing independent calculations on each variant, and combining the outputs afterward during TTA.

Our approach is a generalization of that idea, in the sense that the branching point is located inside the network – the schema is shown in Figure 1. Before that point, the input is run through the network in a standard way. When it reaches a branching point, multiple variants of the data are created that are the result of various augmentation-like transformations on the output from the previous layer. Then, each variant is run through the remaining part of the network independently. Just like with standard augmentation, all of those branches share their weights.

The process can be applied either for training the network or during inference, effectively simulating both data augmentation and test-time augmentation. For inference, in particular, results from all the branches are combined to create a single output. For training, each output can be treated separately.

Our contributions include:

• Exploration of the problem of time-consuming test-time augmentation and introduction of a new method better suited to such scenarios.
• Analysis of the impact of the layer depth at which augmentations are performed on the overall performance with a trade-off between accuracy and computational time.
• A new architecture that achieves results superior to baselines.
• Combining our techniques with test-time augmentation to further boost accuracy.

II. RELATED WORK

Augmentation. Already in 1998, LeCun et al. used artificially distorted images to augment their training set for LeNet [1]. Later, Krizhevsky et al., while introducing the convolutional neural network AlexNet [2] for image recognition on the ImageNet dataset [13], used data augmentation techniques to help prevent overfitting and improve the accuracy. Specifically, they employed translations and horizontal reflections on patches extracted from a given input image to increase their effective training set by a factor of 2048 through the addition of interdependent derivatives of the original image. They also employed PCA on the RGB channels to help their network’s predictions be invariant to changing color or intensity of illumination.

The augmentation techniques developed for image classification also found a use in other computer vision tasks, such as semantic segmentation [14], [15], as well as object detection [16], [17], [18], [19].

Generative adversarial networks (GANs) are also commonly used in a manner similar to data augmentation, especially in
medical tasks. GANs are useful in particular for denoising [20], super-resolution [21] as well as image synthesis [22], [23], [24], [25].

**Feature space augmentation.** Feature space augmentation is a technique that performs data augmentation on intermediate representations. It consists of isolating low dimensional intermediate representations from a portion of the network, and using them to create a better model.

DeVries and Taylor [26] use an LSTM-based sequence autoencoder to arrive at a generic method, which proceeds as follows: first, each sample is encoded, then the resulting representation gets subjected either to added Gaussian noise, or gets combined with its $k$-nearest neighbors in the feature space and in order to interpolate or extrapolate synthetic representations, the authors find as raw input for different learning tasks, or passed through the decoder to generate artificial input data. The authors find an improvement in accuracy on the MNIST and CIFAR-10 datasets.

Moreover, Wong et al. [27] found traditional input space augmentation to outperform feature space augmentation on MNIST not only for convolutional neural networks but also for convolutional support vector machines and convolutional extreme learning machines, with the improvement from using elastic deformation for augmenting the input space being surpassed only by adding real samples.

In HoloGAN [28], the idea of transforming the intermediate representation is used to generate new views of the same scene, by applying rigid transformations to existing 3D features.

DropBlock [29], which can be regarded as a feature space augmentation variant of Cutout [30], transforms feature maps by zeroing out a contiguous region of a given feature map.

In this paper, we explore augmentation in the feature space by transforming intermediate features in a way similar to data augmentation.

**Speed-accuracy trade-off.** There are many works that try to optimize speed and latency while still preserving good accuracy. Mobile architectures [31], [32], [33], [34], [35], [36] were designed for devices that have lackluster computational power. Distillation methods [37] and pruning methods were also proposed as a means of making network calculations faster. Many of the most accurate object detection architectures [17], [18], [38], [39], [40] have difficulties running in realtime with low latency and high FPS. Because of that, faster but less accurate alternatives were created [41], [19]. Many neural architecture search (NAS) methods were also proposed to automatically search for the best architecture given specific speed requirements [42], [43], [44], [45]. Since the computational requirements of our techniques can be freely adjusted, our methods allow both for adjusting the speed and accuracy in computationally limited environments, as well as for improving accuracy in cases when it is more important than speed.

### III. Method

#### A. Method Formulation

A convolutional network can be defined as a function $\mathcal{N}$

\[
\mathcal{N} : \mathbb{R}^{N_1 \times H_0 \times W_0 \times C_0} \rightarrow \mathbb{R}^{1 \times H_k \times W_k \times C_k}
\]

where $\mathcal{N}(X) = (\mathcal{F}_2 \circ \ldots \circ \mathcal{F}_1)(X) = \bigcirc_{i=1...k} \mathcal{F}_i(X)$

We define a Branched Convolutional Network (or simply a branched network) as

\[
\mathcal{B} : \mathbb{R}^{N_1 \times H_0 \times W_0 \times C_0} \rightarrow \mathbb{R}^{R \times H_k \times W_k \times C_k}
\]

where $\mathcal{B}(X) = \bigcup_{i=1...k} (\mathcal{A}_i \circ \mathcal{F}_i)(X)$

Details about the set of transformations used are included in Section III.A3.

A Branched Convolutional Network is a generalization of a regular convolutional network that can return multiple variants of feature maps. Because of that, adjustments have to be made to the training and inference process.

1for simplicity we assume batch size equals 1
1. **Training and Inference:** Let $X$ be an input image, and $(Y_1,\ldots,Y_R) = B(X)$. Let $H$ be the head of the network (i.e. the function that performs the final regression based on the feature map, e.g. in classification problem it outputs the vector of probabilities for all classes), and $P_i = H(Y_i)$.

**Training:** Let $\text{criterion}$ be a criterion function (e.g. cross-entropy), and $T$ be the ground truth for that criterion function.

We use two main ways of calculating loss:

- $\text{loss} = \sum_{i=1}^{k} \text{criterion}(P_i, T)$ - loss is applied independently to every branch and then averaged. In experiments we will refer to it as **none reduction**.

- $\text{loss} = \text{criterion} (\text{reduction} (\{P_i\mid i = 1\ldots k\}, T))$ - We reduce outputs of branches using one of the methods described in Section III-A2 (e.g. $\text{max}$), and then apply the $\text{criterion}$ to the reduced output and the ground truth.

**Inference:** Like in the second method for training we arrive at the output by reducing across all branches, i.e. $\text{output} = \text{reduction} (\{P_i\mid i = 1\ldots k\})$.

2. **Reductions:** In most of our experiments we use $\text{max}$, $\text{sum}$, and $\text{geo}$ – respectively taking maximum, arithmetic mean or geometric mean for each class independently from all branches. Note about naming: after applying the reduction, we normalize the resulting class probability vector. As a result, summing before normalizing gives us the arithmetic mean.

Applying $\text{geo}$ reduction on the probability vector is the same as the arithmetic mean of the logits, if we calculate the probability vector as the softmax of the logits, since $\exp \left( \sum_{i=1}^{k} P_i \right) / \sum_{i=1}^{k} \exp (P_i)$.

3. **Inside-augmentation:** The augmentations we perform are $\text{flip}$, rotation, and scale. For every transformation, we keep the dimensions of the feature map. $\text{flip}$ consists of flipping feature maps horizontally. For zooming out, we pad the remaining part with zeros, and for zooming in, we crop the scaled feature maps. We use bilinear interpolation. We focus mostly on $\text{flip}$ as we are able to obtain the best results from it.

### IV. Experiments

**A. CIFAR-100**

We conduct image classification experiments on the CIFAR-100 [46] dataset. We use the PreAct ResNet-110 [47] architecture. All experiments are run for 180 epochs with 128 images per minibatch. The learning rate starts at 0.1, and is divided by 10 after 82, 123 epoch and by 5 after 160 epoch. The optimizer we use is SGD with 0.9 momentum. Weight decay is set to $2 \cdot 10^{-4}$. The slowdown was measured on an NVIDIA GTX 1080 Ti GPU.

vanilla is the baseline configuration without our method. $\text{vanilla-tta-red}$ is a baseline configuration with standard horizontal flip test-time augmentation with the reduction specified as $\text{red}$. $\text{flip-n-red}$ is a configuration using our method with the $\text{flip}$ inside-augmentation branching on each of the last $n$ feature maps before the last convolution (which results in $2^n$ final feature map variants) and using reduction $\text{red}$ during both training and inference. Adding -tta means combining our method with standard test-time augmentation.

We summarize our results in Figure 2.

**B. ImageNet**

Next, we do experiments on ImageNet-2012. We use ResNet-18 [6]. We train for 105 epochs with a batch size of 256. The learning rate starts at 0.1 and gets divided by 10 at epochs 30, 60, 90, 100. We use a weight decay of $10^{-4}$. For augmentation, we follow Krizhevsky et al. [2] and additionally use random brightness, contrast, and saturation with a coefficient of 0.4. The optimizer we use is SGD with 0.9 momentum with Nesterov’s accelerated gradient.

The naming scheme for configurations is the same as in the previous section. Additionally, we perform experiments where the reduction used in training and inference can differ. For instance $\text{max, sum}$ reduction means $\text{max}$ during training but $\text{sum}$ during inference. $\text{flip-only2-red}$ branches only at the second to last feature map.

The results are summarized in Figure 3.

**C. Inside-impact**

To better understand the intermediate features of the network, we measure a quality which we call **inside-impact**. For every potential spot where an inside-augmentation could be performed in the network, we measure how much transforming the intermediate features in that spot affects accuracy.

We focus on two separate types of inside-impact measurements. **Inference inside-impact** tells us how transforming the features only in a given spot inside the network affects accuracy, assuming that the network was trained without any transformations. We do not branch inside the network. We only transform the feature map once at a given spot.

**Training inside-impact** tells us what accuracy we obtain when augmenting features in a given spot both during training and during inference. We branch into two separate batches at that point, augmenting both of them, and reducing them during inference. All experiments were trained in the way described in Sections IV-A and IV-B.

In inference inside-impact experiments, we use rotation by $15^\circ$ and 10% scale for zooming in and out. We summarize our experiments in Figures 4 and 5. We observe the convolutional filters in the first layers are very flip dependent, i.e. they correspond to the specific side of the object. The deeper the intermediate representation is, the more invariant it gets to changes. The filters in the first layers at the given resolution (i.e. after pooling layers) are much more sensitive to changes.

In training inside-impact experiments, for rotation during the training, the feature map is rotated by a uniformly random...
angle in the range $[-20^\circ, 20^\circ]$ independently in both branches, and during the inference, one branch is not changed and the second is rotated by $15^\circ$. Similarly, for scale, during the training, the feature map is scaled by a uniformly random scale in the range $[0.8, 1.25]$ independently in both branches, and during inference one branch is not changed and the second one is scaled non-deterministically by a scale from the same range as in training.

Figure 6 shows the results. Flip is the most beneficial augmentation. All three augmentations improve when a shallower feature map is tested, together with increasing computational overhead, which allows for a very smooth speed-accuracy trade-off adjustment.

D. Various Reduction Methods

To compare how different reduction methods perform, we ran a series of experiments assuming different reduction methods independently for training and inference and inspecting the error rate. We summarize our findings on CIFAR-100 in Figure 7 and for ImageNet in Figure 8. When training with max, for inference sum appears to be a safe default. When training with none, the best choice is geo. The results from the IV-C Section show that max training reduction performs better in the later layers but does not perform well at the beginning and in the middle of the network where none should be used instead.

V. Conclusion

We propose a feature space augmentation method that applies transformations similar to data augmentation for computer vision to intermediate representations inside the convo-
Fig. 4. Inference inside-impact of an unmodified PreAct ResNet-110 on CIFAR-100. Before \( n \) marks the feature map before the \( n \)-th pooling layer of the network (specific for the architecture used). Inside-augmentations at the beginning of the network have much bigger negative impact on the accuracy.

![Fig. 4. Inference inside-impact of an unmodified PreAct ResNet-110 on CIFAR-100. Before \( n \) marks the feature map before the \( n \)-th pooling layer of the network (specific for the architecture used). Inside-augmentations at the beginning of the network have much bigger negative impact on the accuracy.](image)

We study the inside-impact of the transformations applied to intermediate features in different parts of the network. The network is more sensitive at the beginning, especially to flips, and becomes progressively less sensitive closer to the end. Similarly, applying an inside-augmentation at the beginning of the network may lead to a bigger improvement, but also to more significant computational overhead. The results from these experiments can also be a tool to gain a better understanding of the intermediate representations learned by the network.

We also study different reduction functions for both training and inference. We find that a safe default is to train with \( \text{max} \) and infer with \( \text{sum} \) when deeper features are being transformed, or to train with \( \text{none} \) and infer with \( \text{geo} \) otherwise.

Fig. 5. Inference inside-impact for \textit{flip} using unmodified ResNet-18 on ImageNet. The plot looks consistent with \textit{flip} experiments presented in Figure 4 but is smoother and more contrasting in terms of accuracy. The last two points give the same error rate, since global pooling is invariant to flips.

![Fig. 5. Inference inside-impact for \textit{flip} using unmodified ResNet-18 on ImageNet. The plot looks consistent with \textit{flip} experiments presented in Figure 4 but is smoother and more contrasting in terms of accuracy. The last two points give the same error rate, since global pooling is invariant to flips.](image)

VI. ACKNOWLEDGEMENTS

This work is an extension of research conducted as part of our Bachelor thesis at the University of Warsaw, which was coauthored by our colleagues Eryk Kijewski and Uladzislau Sobal, with help from Krzysztof Ciebiera.
Fig. 6. Training inside-impact on the CIFAR-100 dataset using PreAct ResNet-56. Early in the network, configurations with none, geo perform better than near the end. When using flip-max, the situation is reversed as it performs a little better near the end of the network, slightly outperforming other configurations.

Inference
Training
vanilla max sum geo
vanilla 26.61 26.64 26.62 26.69
none 26.40 26.39 26.40 26.40
max 28.27 25.88 25.93 26.95
sum 26.44 26.40 26.41 26.41
geo 26.55 26.53 26.55 26.55

Fig. 7. Mean error rate on CIFAR-100 using PreAct ResNet-110 with flip-3 augmentation and various ensembling functions for training and inference. Networks trained with none, sum or geo perform very similarly for different inference reductions. Training with max is different and leads to the best results with max or sum during inference.

Inference
Training
vanilla-tta 29.63 29.26 28.97 28.84
flip-3-max 37.86 29.23 28.88 32.44
flip-only2-max 31.16 29.49 29.27 29.51
flip-3-none 29.46 29.29 29.18 29.18
flip-only2-none 29.61 29.48 29.36 29.28

Fig. 8. Mean top1 error rate on ImageNet using ResNet-18 with different augmentations and various reductions during inference. Colors in each row are scaled independently to compare different inference reductions across varied training configurations and not the configurations themselves. When training with none reduction, both geo and sum perform well, while training with max reduction, sum is the best for inference and is also noticeably better than the others.

REFERENCES
[1] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” in Proceedings of the IEEE, 1998, pp. 2278–2324.
[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in Neural Information Processing Systems 25, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, Eds., Curran Associates, Inc., 2012, pp. 1097–1105. [Online]. Available: http://papers.nips.cc/paper/1373-imagenet-classification-with-deep-convolutional-neural-networks.pdf
[3] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” 2015. [ArXiv:1512.03385]
[4] S. Zagoruyko and N. Komodakis, “Wide residual networks,” CoRR, vol. abs/1605.07146, 2016. [Online]. Available: http://arxiv.org/abs/1605.07146
[5] S. Xie, R. Girshick, P. Dollár, Z. Tu, and K. He, “Aggregated residual transformations for deep neural networks,” arXiv preprint arXiv:1611.05431, 2016.
[6] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the inception architecture for computer vision,” CoRR, vol. abs/1512.03567, 2015. [Online]. Available: http://arxiv.org/abs/1512.03567
[7] F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” CoRR, vol. abs/1610.02357, 2016. [Online]. Available: http://arxiv.org/abs/1610.02357
[8] J. Hu, L. Shen, and G. Sun, “Squeeze-and-excitation networks,” CoRR, vol. abs/1709.01507, 2017. [Online]. Available: http://arxiv.org/abs/1709.01507
[9] G. Huang, Z. Liu, and K. Q. Weinberger, “Densely connected convolutional networks,” CoRR, vol. abs/1608.06993, 2016. [Online]. Available: http://arxiv.org/abs/1608.06993
[10] D. E. Worrall, S. J. Garbin, D. Turmukhambetov, and G. J. Brostow, “Harmonic networks: Deep translation and rotation equivariance,” CoRR, vol. abs/1612.04642, 2016. [Online]. Available: http://arxiv.org/abs/1612.04642
[11] Y. Wu, A. Kirillow, F. Massa, W.-Y. Lo, and R. Girshick, “Detectron2,” https://github.com/facebookresearch/detectron2, 2019.
[12] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings, Y. Bengio and Y. LeCun, Eds., 2015. [Online]. Available: http://arxiv.org/abs/1409.1556
[13] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. S. Bernstein, A. C. Berg, and F. Li, “ImageNet large scale visual recognition challenge,” CoRR, vol. abs/1409.0575, 2014. [Online]. Available: http://arxiv.org/abs/1409.0575
[14] J. Long, E. Shelhamer, and T. Darrell, “Fully convolutional networks for semantic segmentation,” CoRR, vol. abs/1411.4038, 2014. [Online]. Available: http://arxiv.org/abs/1411.4038
[15] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” CoRR, vol. abs/1505.04597, 2015. [Online]. Available: http://arxiv.org/abs/1505.04597
[16] R. Girshick, J. Donahue, T. Darrell, and J. Malik, “Rich feature
A few sentences from the text:

- "Biomedical data augmentation using generative adversarial neural networks," 10 2017, pp. 626–634.
- "How to fool radiologists with generative adversarial networks? A visual Turing test for lung cancer diagnosis," CoRR, vol. abs/1710.09762, 2017. [Online]. Available: http://arxiv.org/abs/1710.09762
- "Synthetic data augmentation using GAN for improved liver lesion classification," CoRR, vol. abs/1801.02385, 2018. [Online]. Available: http://arxiv.org/abs/1801.02385
- "Dataset augmentation in feature space," vol. 1702.05538, 2017. [Online]. Available: http://arxiv.org/abs/1702.05538
- "Understanding data augmentation for classification: when to warp?" CoRR, vol. abs/1609.08764, 2016. [Online]. Available: http://arxiv.org/abs/1609.08764
- "Dropblock: A regularization method for convolutional networks," CoRR, vol. abs/1810.12900, 2018. [Online]. Available: http://arxiv.org/abs/1810.12900
- "Improved regularization of convolutional neural networks with cutout," CoRR, vol. abs/1801.09392, 2018. [Online]. Available: http://arxiv.org/abs/1801.09392
- "ShuffleNet: An extremely efficient convolutional neural network for mobile devices," CoRR, vol. abs/1707.01083, 2017. [Online]. Available: http://arxiv.org/abs/1707.01083
- "Shufflenet V2: practical guidelines for efficient CNN architecture design," CoRR, vol. abs/1807.11164, 2018. [Online]. Available: http://arxiv.org/abs/1807.11164
- "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <1mb model size," CoRR, vol. abs/1602.07360, 2016. [Online]. Available: http://arxiv.org/abs/1602.07360
- "Distilling the knowledge in a neural network," vol. abs/1503.02531, 2015. [Online]. Available: http://arxiv.org/abs/1503.02531