This is the accepted version of a paper presented at International Conference on Machine Learning (ICML) Workshops, 2019 Workshop on Uncertainty and Robustness in Deep Learning.

Citation for the original published paper:

Efficient Evaluation-Time Uncertainty Estimation by Improved Distillation
In:

N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-260511
Efficient Evaluation-Time Uncertainty Estimation by Improved Distillation

Erik Englesson 1 Hossein Azizpour 1

Abstract

In this work we aim to obtain computationally-efficient uncertainty estimates with deep networks. For this, we propose a modified knowledge distillation procedure that achieves state-of-the-art uncertainty estimates both for in and out-of-distribution samples. Our contributions include a) demonstrating and adapting to distillation’s regularization effect b) proposing a novel target teacher distribution c) a simple augmentation procedure to improve out-of-distribution uncertainty estimates d) shedding light on the distillation procedure through comprehensive set of experiments.

1. Introduction

Deep neural networks are increasingly used in real-world applications thanks to their impressive accuracy. Nevertheless, many of these applications involve human users which necessitate high level of transparency and trust beside the accuracy. A crucial ingredient to enable trust, is to associate the automatic decision with a calibrated uncertainty. Different techniques have been developed to obtain uncertainty estimation from deep networks including Bayesian modeling using variational approximation (Graves, 2011), expectation propagation (Hernández-Lobato & Adams, 2015), sampling (Gong et al., 2018) and non-Bayesian methods such as bootstrapping (Lakshminarayanan et al., 2017) and classification margin (Geifman & El-Yaniv, 2017).

While many of those models achieve acceptable uncertainty estimates (Lakshminarayanan et al., 2017), they are notoriously slow to train and evaluate which makes them non-viable for real-world implementation. Methods have been developed to expedite the training process. (Gal & Ghahramani, 2016; Teye et al., 2018) cast standard deep networks as approximate Bayesian inference. (Welling & Teh, 2011) use Langevin dynamics in tandem with stochastic gradient descent, and (Huang et al., 2017) employ the training snapshots to avoid sampling and/or multiple training runs.

All these techniques effectively improve the computational complexity of training, but remain prohibitively expensive at evaluation, essentially due to the multiple inference required for uncertainty estimates at test time. This is despite the fact that computational and memory-footprint is of high concern for real-world applications where the evaluation model needs to be deployed in products with limited computational and memory capacity.

The focus of this work is to address this issue. We devise an algorithm to efficiently obtain uncertainty estimates at evaluation time irrespective of the modelling choice. Common deep networks for epistemic uncertainty produces either samples of the posterior $P(\theta|D)$ or a parametric approximation of it $q_\omega(\theta)$, where $\theta \in \Theta$ is the model parameters (i.e. weights and biases of the network), $D = \{(x_i, y_i)\}_{i=1}^{N}$ the training data, and $\omega$ the parameters of the approximating distribution. To marginalize over the parameter uncertainty, usually, $m$ samples of the parameters $\{\theta_1, \ldots, \theta_m\}$ are obtained e.g. through bootstrapping (Lakshminarayanan et al., 2017) or sampling of $q_\omega(\theta)$ (Gal & Ghahramani, 2016):

$$P(y|x, D) \approx \frac{1}{m} \sum_{i=1}^{m} P(y|x, \theta_i), \quad \{\theta_i\} \sim P(\theta|D). \quad (1)$$

This summation is the source of evaluation memory/time complexity. In this work, we aim to train a single deep network with parameters $\theta'$ potentially from a different parameter space $\Theta'$ that minimizes a divergence from the mean distribution of Eq 1 for all $x$. The teacher-student setup of (Hinton et al., 2015) is suitable for this purpose.

2. Method

Our goal is to optimize the parameters of a single (student) network $\theta'$ to produce class-posterior similar to our target (teacher) distribution for both in and out-of-distribution samples. One measure is the KL-divergence:

$$\min_{\theta'} \sum_{x \in X} D_{KL}(P(y|x, D) || P(y|x, \theta')) \quad (2)$$

with $X$ being student training set, and $P(y|x, D)$ is approximated as in Eq 1. We denote this training procedure as vanilla distillation. Note that Eq 2 exclude the hyperparameters of the standard distillation (Hinton et al., 2015): temperature $T$ and mixing parameter $\alpha$. 

---

1RPL, KTH, Stockholm, Sweden. Correspondence to: Erik Englesson <engless@kth.se>.

Presented at the ICML 2019 Workshop on Uncertainty and Robustness in Deep Learning. Copyright 2019 by the author(s).
2.1. Target distribution as regularization

The student needs to learn a dispersed distribution as target in contrast to the teacher’s hard label (i.e. Kronecker delta pmf, \(\delta_{y,y_i}\)), which we assume is a “more difficult” task that requires higher model capacity. Indeed, we have empirically observed that students, with the same architecture as the teacher, tend to converge slower and are less prone to overfitting. Furthermore, (Hinton et al., 2015) and (Balan et al., 2015) noticed a lower L2 regularization weight is needed for the student. Based on these observations, we propose the following two modifications to standard distillation.

Higher capacity students. One way to address this phenomenon is to increase the student’s capacity (w.r.t. teacher) to account for the additional complexity. That is, we assume \(|\Theta'| > |\Theta|\). This can be done, for instance, by increasing the depth or width of the student network. \(^1\)

Sharper target distribution. Alternatively, for each sample, we can decrease target’s entropy \(H(\cdot)\) by sharpening the teacher’s distribution \(p\) to a new target distribution \(q\):

\[
q = (1-\alpha)p + \alpha r
\]

with \(H(r) < H(p)\), \(\arg\max_y r = \arg\max_y p\), \(0 < \alpha < 1\).

\[r = \delta_{y,y_i}\] gives the formulation of knowledge distillation without temperature \(T\). This can explain the improvement (Hinton et al., 2015) observed by adding the true labels to the distribution for the correctly classified examples.

2.2. Proper class-posterior distribution

Here we pose the question of whether to follow the teacher even when it makes wrong decisions (i.e. \(y_{\text{max}} \neq y_i\), where \(y_{\text{max}} \triangleq \arg\max_y p_i(y)\)). From the perspective of predictive uncertainty, we argue that it is only reasonable for a target distribution to be as “faulty” as a uniform distribution. However, a uniform distribution loses the dark knowledge in the wrong prediction, so we propose the following alternative distribution for each misclassified sample \(i\):

\[
q_i = (1-\alpha_i)p_i + \alpha_i \delta_{y_i,y_i} \text{ with } \frac{p_i(y_{\text{max}})}{p_i(y_{\text{max}})+\sum_{y \neq y_{\text{max}}} p_i(y)} < \alpha_i \leq 1.
\]

\(\alpha\) at its minimum makes a new target distribution \(q\) with maximum mass on the correct class while still retaining maximal mass on non-correct classes and thereby dark knowledge. This complements the previous argument by explaining the observed improvement in (Hinton et al., 2015) of mixing in the true labels for the wrongly classified examples.

2.3. Robustness to out-of-distribution (OOD) samples

Ideally we want the model to have high uncertainty when it is presented with samples that are out of the training distribution, i.e., \(O = \{x|P(x,y) \approx 0 \ \forall y \in \mathcal{Y}\}\).\(^2\) We posit that this set includes two important subsets.

Natural set. OOD samples can come from the support of \(P(x)\), i.e., \(O_{\text{natural}} = \{x|P(x) > \epsilon\} \cap O\). For instance, an image of a car is a natural OOD sample for a cat vs dog classification task. (Li & Hoiem, 2018) uses a large unlabeled student training dataset for this purpose.

Unnatural set. Unnatural OOD samples come from the rest of the space, i.e., \(O_{\text{unnatural}} = \{x|P(x) \approx 0\}\) which are important for defending against adversarial attacks. (Lakshminarayanan et al., 2017) uses adversarial training to become robust to this set of OOD samples.

3. Contributions

The contributions of this work can be summarized as:

- we recognize the regularization effect of dispersed target distributions and accordingly suggest techniques to improve the distillation process
- we provide justification for the particular target distribution of standard distillation in (Hinton et al., 2015)
- we propose a simple and yet effective technique for distillation of out-of-distribution predictive uncertainty
- we conduct a comprehensive set of experiments and evaluations to study the aforementioned aspects

4. Related Work

Here we briefly present the recent works that address the computational efficiency of evaluating predictive uncertainty and delineate our work with respect to them. (Hinton et al., 2015) coined knowledge distillation to summarize an ensemble. They focused on the accuracy of the student and not the uncertainty estimates. Our work sheds light on their design choices and is more elaborately designed for the purpose of uncertainty distillation. (Li & Hoiem, 2018; Gurau et al., 2018; Balan et al., 2015) are the closest to our work, they use (Hinton et al., 2015) to distill ensemble networks, Monte Carlo sampling of dropout networks (Gal & Ghahramani, 2016) and approximate posterior samples of SGLD (Welling & Teh, 2011) respectively. They use distillation in its standard form, thus our observations and proposed modifications are complementary to those works. (Li & Hoiem, 2018) addresses the problem of OOD prediction with an unlabeled dataset, whereas we propose different and potentially complementary procedures.

\(^{1}\)Although this results into a less efficient student, it will still be eminently more efficient than evaluating multiple teachers. Also, the student, after being fully trained, can be compressed using various existing approaches (e.g. (Zhuang et al., 2018)).

\(^{2}\)Note that, marginalizing over \(y \in \mathcal{Y}\) does not give \(P(x)\) since \(\mathcal{Y}\) is limited to the current task excluding a “negative” class.
Figure 1. Evaluation of the predictive uncertainty for a) in-distribution and b) out-of-distribution samples. Models are trained on CIFAR-10 with vanilla distillation (standard distillation with $\alpha = 0$, $T = 1$). For the in-distribution plot, we vary the ensemble size. The student is trained on a teacher with the corresponding number of networks. Student and teacher networks have the same capacity (depth 9). For out-of-distribution, we evaluate the models on SVHN and create a histogram over the entropy of the predicted distributions. The quality of the predictive uncertainty is decent for the in-distribution, but there is room for improvement for out-of-distribution samples.

(Anil et al., 2018) designs a technique to distill ensembles in an online fashion, focused on a distributed training scenario. Their goal is to match and improve the accuracy as opposed to predictive uncertainty.

Finally, (Wu et al., 2019) proposes a method to deterministically propagate uncertainty of model parameters and activations to the output layer. While this elegant approach circumvents the computational burden of sampling the parameter posterior, it achieves inferior results compared to the ensemble model of (Lakshminarayanan et al., 2017).

5. Experiments

We use the state-of-the-art ensemble technique proposed in (Lakshminarayanan et al., 2017) as the teacher. We measure calibration of in-distribution predictive uncertainty through negative log-likelihood (NLL) and Brier score. We evaluate the robustness to OOD samples via entropy histograms. The experimental results of the student are reported as the mean and std of 5 runs unless stated otherwise. We use CIFAR10 as the main dataset, and report some results on MNIST and CIFAR100. See appendix Sec A for details.

5.1. Vanilla distillation

First, we show that vanilla distillation produces decent predictive uncertainty for the in-distribution samples, while it is significantly worse on the OOD samples, see Fig 1. Results for other network depths are in Fig 4 in the appendix. In Fig 1(b), we can see that the student is more over-confident in its predictions compared to the teacher. It is still interesting that this simple baseline without hyperparameters performs on-par with the ensemble teacher. We now further improve upon these results using our proposed techniques.

5.2. Target distribution as regularization

We have observed that the teachers quickly overfit to NLL after the first drop in learning rate (while accuracy still improves (Guo et al., 2017)); this behavior, however, is not observed for the students. Furthermore, the convergence time of the students is far longer than the teachers – 2500 vs 85 epochs. These observations hint that the student learning process is more regularized than its teacher’s counterpart. In the following, we take measures based on this observation.

Higher capacity students. Fig 2(a) serves as a baseline for how the teacher performs for varying number of networks and network depths. In Fig 2(b) we consistently observe better NLL as the student’s depth is increased. The results for other teacher depths are shown in Fig 5 in the appendix. More interestingly, increasing the student’s capacity is more effective than increasing the teacher’s, see Fig 2(c). This can be due to the same regularization effect. This was also observed for students of depth 5 and 18, see appendix Fig 6.

Finally, all the figures crucially indicate that the improvement in student performance by increased depth is not merely because the original task demanded larger networks. That can be seen by comparing the improvements in the ensemble performance to student’s as the depth increases.

Sharpening the target distribution. Another way to address the regularization of dispersed target distributions is to lower the entropy as in (Hinton et al., 2015). Interestingly, we empirically observed the effect of $\alpha$ diminishes as the capacity of the student is increased. Appendix Tab 1 shows that a student of depth 18 trained using a teacher of depth 5, does not significantly benefit from an increase in $\alpha$. For results of sharpened targets on MNIST and CIFAR100, see Appendix Fig 7 and Tab 3, respectively.

5.3. Proper class-posterior distribution

As we discussed, a way to improve the distillation process is to correct for the wrong predictions of the teacher ensemble. We proposed another interpretation of the weighted average between the true label and the teacher predictions. We move $\alpha_i$ in Eq 4 in the range $p(y_{max}) - p(y_i) / p(y_{max}) + p(y_i) < \alpha_i \leq 1$. We observed no significant difference when using the approach on CIFAR10, however, it gives small improvements on CIFAR100 (Tab 2 in the appendix). We hypothesize the reason
for this is that the number of misclassified examples was too low for CIFAR10 for the change to show significant improvement and thus going to a more challenging task such as ImageNet would further signify the benefits.

5.4. Robustness to out-of-distribution samples

In Fig 2, we saw that the uncertainty estimates for in-distribution samples are on par with the ensemble, especially with increased student’s capacity while Fig 1 shows the robustness to OOD samples is far from ideal. We propose a simple approach for the natural OOD samples. Here we simply perturb the samples of the natural manifold by applying image transformations that do not violate the manifold including cropping and mirroring. In the standard case, the label for an augmented image is the teacher’s prediction for the corresponding unperturbed image. We instead propose to use the teacher’s prediction on the augmented image as the label, providing more information about the teacher during training. Fig 3 shows the intriguing improvement this simple technique brings. The noticeable improvements we get from this simple approach, highlights the promise of pursuing this direction further. Interestingly, we have found that more aggressive transformations which is usually harmful for standard training helps the teacher-student learning.

6. Final remarks

In this work we closely analyzed the distillation process of (Hinton et al., 2015) from an uncertainty estimation perspective. We shed light on their design choices which resulted into suggesting additional improvements. In the experimental part of this work we empirically studied the suggested aspects which led to many interesting observations. Throughout all the experiments we tried to keep high-level experimental standard in our reports by cross-validated hyperparameter optimisation for baseline students. We also reported values as result of 5 different runs. Important future directions include theoretical analysis of our observations regarding the effects of distillation and its design choices and applying the techniques on larger datasets such as ImageNet to further highlight their effectiveness.

Acknowledgements

This work was supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP-AI/MLX) funded by the Knut and Alice Wallenberg Foundation.

Figure 2. Capacity and ensemble size of teachers vs corresponding students on CIFAR-10: Figure (a) shows how the performance of the teacher depends on the number of networks and the capacity of each network. The performance of the student is consistently improved by increased depth(b), while the depth of the networks in the teacher does not significantly affect the student(c). All students are trained using vanilla distillation.

Figure 3. Out-of-Distribution: Entropy histograms of the predictions of models trained on CIFAR datasets and evaluated on OOD SVHN dataset. Student corresponds to training with sharper targets through interpolation with true delta distribution, Student-Aug uses transformations to traverse the natural manifold. The teacher uses 15 networks of depth 5(a) or depth 18(b) and the students uses the same depth as their teacher.
References


Li, Z. and Hoiem, D. Reducing overconfident errors outside the known distribution. 2018.


A. Experimental Details

We evaluate our method on MNIST, CIFAR-10 and CIFAR-100 training a dense neural network on MNIST and ResNet variants for CIFAR. To simplify things, we only consider ensembles of networks where each network has the same capacity.

All models are trained on a train-validation split, where hyperparameters are optimized on the validation set based on NLL. We do not retrain on the entire training set before evaluating on the test set.

MNIST For all MNIST experiments, we use the same dense neural network architecture as proposed in (Lakshminarayanan et al., 2017). That is, three hidden layers with 200 units per layer, ReLU activations and batch normalization. Both the student and the teacher is trained using the Adam optimizer. Each network of the teacher is trained for 10 epochs with a fixed learning rate of 0.001 and a batch size of 1000. The students are trained for 600 epochs with a fixed learning rate of 0.002 and a batch size of 64.

CIFAR For all CIFAR-10 and CIFAR-100 experiments, we use the ResNet version proposed by (He et al., 2016). We use ResNet models of varying depth 5(ResNet32), 9(ResNet56), 18(ResNet110), etc. We train these models using the Momentum optimizer with a batch size of 128 and a learning rate of 0.1. The teacher networks overfit quickly to NLL after the first drop in learning rate. We drop the learning rate at epoch 82 and do early stopping at epoch 85 before the validation NLL degrades. The students can be trained for longer without overfitting to NLL. We use 2500 epochs and the learning rate is reduced by a factor of 10 at epoch 2000, 2100, 2300. For data augmentation we use padding, random cropping and horizontal flips. As the baseline, the label for each augmented image is the prediction of the teacher on the corresponding original image. For the improved augmentation technique, the label for each augmented image is the prediction of the teacher for that particular augmented image.

B. Additional Figures and Tables

Table 1. Sharpening the target distribution for CIFAR-10: An ensemble of 15 teachers with depth 5 is distilled to a student of depth 18 with varying $\alpha$ in order to sharpen the target distributions. However, we see that as the student capacity is already addressing the regularization effect caused by the dispersed target distribution, the importance of $\alpha$ is diminished.

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>NLL_{mean}</th>
<th>NLL_{std}</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>0.1573</td>
<td>0.0016</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1575</td>
<td>0.0016</td>
</tr>
<tr>
<td>0.2</td>
<td>0.1575</td>
<td>0.0014</td>
</tr>
<tr>
<td>0.3</td>
<td>0.1572</td>
<td>0.0012</td>
</tr>
</tbody>
</table>

Table 2. Proper class-posterior distribution for CIFAR-100: An ensemble of 15 teachers with depth 5 is distilled to a student of depth 5. Here we correct the target distribution for the wrongly classified samples by the teacher ensemble. See Eq 4. We vary $\alpha_i$ in the range $\frac{p(y_{max}) - p(y_i)}{p(y_{max}) - p(y_i) + 1} < \alpha_i \leq 1$ which spans the spectrum of dark knowledge preservation constrained on the prediction (argmax) being correct. While the same experiment for CIFAR10 did not show significant improvement, we observe some promise moving to CIFAR100. We posit this is due to the fact that there are only a few wrongly classified samples in CIFAR10 compared to CIFAR100. Consequently, we expect larger improvements when going to more challenging tasks such as ImageNet. Here we denote the lower bound by $\tilde{\alpha}_i \equiv \frac{p(y_{max}) - p(y_i)}{p(y_{max}) - p(y_i) + 1}$.

<table>
<thead>
<tr>
<th>$\alpha_i$, $\tilde{\alpha}_i$, $0.9\tilde{\alpha}_i + 0.1$, $0.8\tilde{\alpha}_i + 0.2$</th>
<th>NLL_{mean}</th>
<th>NLL_{std}</th>
<th>REF_{mean}</th>
<th>REF_{std}</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.920</td>
<td>0.922</td>
<td>0.005</td>
<td>0.003</td>
<td>0.007</td>
</tr>
</tbody>
</table>
Figure 4. **Vanilla distillation for different depths on CIFAR-10:** Evaluating the quality of the predictive uncertainty for the teacher and students trained on CIFAR-10 using vanilla distillation (equivalent to standard distillation with $\alpha = 0, T = 1$). The teacher and student is compared in terms of classification error, NLL and Brier score for varying depths. The teacher and student uses the same depth for their networks.

Figure 5. **Performance impact of student depth on CIFAR-10:** Increasing the depth of the student, while keeping the teacher depth fixed, leads to better NLL. This improvement is observed for teachers of depth 5(a), 9(b) and 18(c). Increasing the depth of the student consistently improves the result, no matter the number/depth of networks used by the teacher.

Figure 6. **Performance impact of teacher depth on CIFAR-10:** Varying the depth of the teacher, while keeping the depth of the student fixed, has no significant effect on the performance of the student. This seems to hold for students of different depths, see (a), (b) and (c). No matter the number of networks used by the teacher, or the depth of the student, varying the depth of the teacher does not significantly affect the student’s performance.
Table 3. In-distribution performance on CIFAR-100: An ensemble of 15 teacher networks of depth 18 is distilled to a student of depth 18. The classification error, NLL, and Brier score for the teacher (baseline) and students of varying depth and mixing parameter $\alpha$. Sharpening the targets ($\alpha > 0$) does not improve the performance, however increasing the depth of the student makes a significant improvement.

<table>
<thead>
<tr>
<th>Depth</th>
<th>$\alpha$</th>
<th>Error</th>
<th>NLL</th>
<th>Brier Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teacher</td>
<td>18</td>
<td>20.95</td>
<td>0.7434</td>
<td>0.00296</td>
</tr>
<tr>
<td>Student</td>
<td>18</td>
<td>0.0</td>
<td>22.92 ± 0.15</td>
<td>0.8187 ± 0.0060</td>
</tr>
<tr>
<td>Student</td>
<td>18</td>
<td>0.1</td>
<td>23.24 ± 0.29</td>
<td>0.8257 ± 0.0049</td>
</tr>
<tr>
<td>Student</td>
<td>27</td>
<td>0.0</td>
<td>22.16 ± 0.15</td>
<td>0.7856 ± 0.0070</td>
</tr>
<tr>
<td>Student</td>
<td>27</td>
<td>0.1</td>
<td>22.26 ± 0.15</td>
<td>0.7923 ± 0.0044</td>
</tr>
</tbody>
</table>

Figure 7. In-distribution quality of uncertainty for MNIST: Evaluating the quality of the predictive uncertainty for the teacher and students trained on MNIST using an alpha of 0.2. The performance is shown for varying number of networks. For the student, this corresponds to how many networks was used by its teacher.