ALM-KD: Knowledge Distillation with noisy labels via adaptive loss mixing

Durga Sivasubramanian\textsuperscript{1,2}, Pradeep Shenoy\textsuperscript{2}, Prathosh AP\textsuperscript{3}, and Ganesh Ramakrishnan\textsuperscript{1}

\textsuperscript{1}Indian Institute of Technology, Bombay
\textsuperscript{2}Google Research, India
\textsuperscript{3}Indian Institute of Science, Bengaluru

February 8, 2022

Abstract

Knowledge distillation is a technique where the outputs of a pretrained model, often known as the teacher model is used for training a student model in a supervised setting. The teacher model outputs being a richer distribution over labels should improve student model’s performance as opposed to training with the usual hard labels. However, the label distribution imposed by the logits of the teacher network may not be always informative, and may lead to poor student performance. We tackle this problem via the use of an adaptive loss mixing scheme during KD. Specifically, our method learns an instance-specific convex combination of the teacher-matching and label supervision objectives, using meta learning on a validation metric signalling to the student ‘how much’ of KD is to be used. Through a range of experiments on controlled synthetic data and real-world datasets we demonstrate performance gains obtained using our approach in the standard KD setting as well as in multi-teacher and self-distillation settings.

1 Introduction

A central challenge for supervised learning from finite data is that the cardinal labels associated with each sample may only provide partial information about the input data. In reality, a given data point may be better described by a distribution over the label space. In these scenarios, a model trained on the entire dataset may output more nuanced ‘soft labels’ for each training input, and using these soft labels as targets for a “student model” may improve the generalization capability of the student. Recent work (Menon et al., 2021) formalizes this notion from a Bayesian perspective; it shows that when one-hot labels are an imperfect representation of the true probability distribution, KD helps in reducing the variance associated with probability estimates in a student model. Other work examines, from an empirical perspective, when and how distillation may improve upon training from scratch on the labels alone. For instance, when the teacher has been overtrained on the training data, it is likely to achieve very low/zero error rates w.r.t. the (incomplete) label loss simply by overfitting on random noise in the dataset; in these circumstances, it is likely that the probabilities output by the teacher do not accurately represent the underlying uncertainty, and students may be led astray. Various empirical approaches try to alleviate this issue, including annealing of the temperature
parameter (Hinton et al., 2015; Wen et al., 2020), and early stopping of teacher training (Cho & Hariharan, 2019). In each of these circumstances, the challenge is that neither the data labels, nor the teacher trained on those labels, are able to effectively capture the underlying soft-label distribution.

We propose ALM-KD, an adaptive loss mixing technique for knowledge distillation, aimed at addressing these challenges. Our proposal is driven by the following key insight: the label associated with each sample in the training data has its own degree of uncertainty, which is not explicitly available to the teacher at training time and which can result in a sub-optimal teacher model. While the teacher can in general add nuanced information over and above the information in the data label, this additional information needs to be regulated on a sample-by-sample basis. To address this, we propose to learn an instance-specific mixing parameter that combines the teacher-matching and supervision objectives, to be used as target for training the student. We devise a meta-learning algorithm, based on a separate validation metric, to estimate these instance-specific parameters in an unbiased manner. We show that our approach produces more accurate student models over a range of datasets and student architectures. We extend our approach to multiple teachers, and demonstrate that our approach effectively identifies more informative teachers, and outperforms recent proposals for multi-teacher KD. Crucially, we also show gains in the self-distillation setting, where the teacher and student have the same architecture, but the student benefits from richer supervision. Here, our approach learns models that are more accurate than the teacher by leveraging KD and instance-specific loss mixing.

Our Contributions:

- ALM-KD: an adaptive knowledge distillation scheme that titrates teacher knowledge and label information on a per-instance basis for effective training of students, and a validation metric based meta-learning scheme for estimating these instance parameters.

- Extensive experiments demonstrating the gains of ALM-KD-trained student models over state-of-the-art KD-trained models, including experiments in the self-distillation setting.

- Detailed analyses of the learnt instance parameters to elucidate the mechanisms by which ALM-KD improves KD learning.

2 Related work

Knowledge distillation (KD (Hinton et al., 2015)) in a supervised learning setting trains a “student” model to mimic the outputs of a larger, pretrained “teacher” model instead of directly training on the supervised signal. The expectations are twofold: that teacher outputs capture more information about instance / label uncertainty (the so-called dark knowledge), and that smaller, more efficient student models can be trained for roughly similar performance using the dark knowledge. Readers are directed to (Gou et al., 2021) for a comprehensive survey of distillation methods and their applications.

Methods for improving distillation: The efficacy of KD can be limited by teacher accuracy (see e.g., (Menon et al., 2021) for some theoretical results), and student representational capacity, among other factors. For instance, Cho & Hariharan (2019) show that early stopped teacher models aid better in training the student models; however, identifying the best possible teacher requires repeating the entire process of distillation multiple times on the student model. Mirzadeh et al. (2019) present an alternative approach, TAKD, by introducing Teacher Assistants (TA) or intermediate models, to bridge the representational gap between the teacher and the student. KD proceeds in multiple steps by transferring signals from the teacher, through TAs to the student. This method does, however, also transfer errors from the higher level to the lower level models. Son et al. (2021)
present a Stochastic approach (DGGK) for simultaneously training all intermediate models with occasional dropout of models. In Liu et al. (2020), multiple teacher networks are used with an intermediate knowledge transfer step using latent distillation. Heo et al. (2019) propose the use of adversarial samples for distillation to increase the robustness.

**Instance hardness and label noise:** The supervised learning literature explores the notion of instance hardness (Zhou et al., 2020a,b), where specific instances in the training data may vary widely in their ease of classification. This insight is used to develop curricula for learning from the right sequence of easy and difficult examples (Zhou et al., 2020b), or instance-specific temperature parameters in supervised learning (Saxena et al., 2019). Other, closely related approaches (Algan & Ulusoy, 2021; Vyas et al., 2020), learn a per-instance label uncertainty parameter to account for potential label noise. In the distillation setting, too, the importance of instance-specific learning has been explored; for instance, Wang et al. (2018a,b), employ adversarial learning for matching the distributions of teacher and student logits, and Zhao et al. (2021) demonstrate the benefits of a learning curriculum on training samples in distillation.

**Our contributions in context:** We propose ALM-KD, a distillation method that adjusts the relative importance of teacher and data label on a per-instance basis. To our knowledge, this is the first proposal for adaptive mixing of distillation loss on a per-instance basis. We propose a meta-learning algorithm that uses validation data for unbiased parameter estimation. Our proposal addresses several issues in KD identified by existing work, such as large teacher-student gaps (Mirzadeh et al., 2019), or the need for early stopping of teacher (Cho & Hariharan, 2019), and can enhance a wide variety of current KD methods since it is an additional dimension of optimization.

While our approach is similar in spirit to the noisy label/instance hardness scenarios, in that instance-specific parameters are learned to counter variability across the data, there are two key differences. First, we employ the powerful distillation framework, thereby replacing a coarse one-dimensional measure of label uncertainty (Saxena et al., 2019; Algan & Ulusoy, 2021) by a rich teacher distribution whose relative importance is then learned from data. In this sense, ALM-KD is a strict generalization of these previous approaches. Second, our results are much more broadly applicable, to scenarios such as self-distillation, to teacher-student settings, and to learning from multiple teachers.

### 3 Problem Formulation

We have a supervised learning setting with a dataset $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^N$ with instances $x_i$ and categorical labels $y_i$. We wish to train a student model which outputs the logits $a^{(S)} = \text{StudentModel}(x)$. Traditionally, we train such a model by optimizing a cross-entropy based loss $L_s$ defined as follows:

$$L_s = H(\text{softmax}(a^{(S)}), y)$$  \hspace{1cm} (1)

Let us say we have access to a pretrained teacher model which outputs the logits $a^{(T)} = \text{TeacherModel}(x)$. We can frame a teacher matching objective for the student as a KL-divergence between the predictions of the student and the teacher:

$$L_{KD} = \tau^2 KL(y^{(S)}, y^{(T)})$$  \hspace{1cm} (2)

Assuming that $\tau$ is a temperature parameter that controls the softening of the KD loss in Eq. (2), we have $y^{(S)} = \text{softmax}\left(\frac{a^{(S)}}{\tau}\right)$ and $y^{(T)} = \text{softmax}\left(\frac{a^{(T)}}{\tau}\right).$
Combining the two objectives, the knowledge distillation loss (Hinton et al., 2015) is defined as follows:

\[
\mathcal{L}_{\text{student}} = (1 - \lambda)\mathcal{L}_s + \lambda\mathcal{L}_{KD}
\]  

(3)

In Eq.(3), the parameter \(\lambda\) determines the tradeoff between the traditional cross-entropy based loss \(\mathcal{L}_s\) and the additional KL-divergence based loss \(\mathcal{L}_{KD}\).

3.1 Effectiveness of Knowledge Distillation

Menon et al. (2021) discuss the bias-variance trade-off associated with the knowledge distillation loss, with a view to identifying the theoretical advantage of distillation over the vanilla cross-entropy loss. They show, in particular, that:

\[
\mathbb{E}[(\tilde{R}(f; S) - R(f))^2] \leq \frac{1}{N} \mathcal{V}[p^T(x)^T \mathcal{L}(\text{softmax}(a^{(S)}))] + \mathcal{O}(\mathbb{E}[p^T(x) - \mathcal{p}^*(x)]^2 + \mathcal{V}[p^T(x)])
\]  

(4)

where \(\tilde{R}(f; S)\) is the distillation risk and \(R(f)\) is the population risk. Further, \((p^T(x) = \text{softmax}(a^{(T)}), \mathcal{p}^*(x))\) represents the (true, unknown) Bayes class probability distribution over the labels, and \(\mathcal{L}\) is the cross-entropy loss over the labels. On the right hand side of the inequality (4), the second term dominates when \(N\) is large; this suggests that the effectiveness of distillation is governed by the variance in teacher model’s predictions, as well as its closeness to the true distribution \(\mathcal{p}^*(x)\). This is the classic bias-variance trade-off, and implies that a teacher model balancing the two would help in better generalisation of the student. Teacher bias can be reduced by increasing the teacher model’s capacity, at the cost of higher variance in prediction. One way to quantify variance is to estimate the difference in training loss and the loss on a validation or held out set; therefore, a good teacher model is one with lower validation error.

3.2 Optimizing the distillation loss

The motivation for our method is drawn from the following Lemma:

**Lemma:** Assuming that the true label posterior \((\mathcal{p}^*(x))\) is not known to the teacher, there exists an optimal \(\lambda\) in Eq.(3), that leads to lower variance in the distilled risk (Proof in the Appendix).

In other words, if we were able to identify the value of this optimal \(\lambda\), we could learn a better student model. Note, however, that the above lemma and its proof do not offer a direct method of estimating the optimal \(\lambda\), although empirical schemes such as grid search could potentially be deployed. This leaves open the question of a principled method of optimizing Eq. (3) for the value of \(\lambda\). On another note, the extensive literature on instance hardness and label noise (see e.g., Zhou et al. (2020b); Algan & Ulusoy (2021); Saxena et al. (2019)) suggest that the relative informativeness of a learned teacher model and the ground-truth data label are also expected to vary widely across instances in real datasets.

Combining these two observations, we are motivated to ask: 1) How can we customize the distillation loss on a per-instance basis? and 2) How can we learn the resulting per-instance parameters in a principled, optimization-driven manner? In Section 4, we present formal answers to these questions in the form of a bi-level optimization criterion, and a meta-learning procedure for solving the optimization objective, respectively.
Algorithm 1 Algorithm for learning $\lambda$s via meta learning

**Require:** Training data $\mathcal{U}$, Validation data $\mathcal{V}$, $\theta^{(0)}$ model parameters initialization, $\tau$: Temperature, $\eta$: learning rate, $\eta_\lambda$: learning rate for updating $\lambda$.

**Require:** $LL_{SL}$ Supervised loss, $LL_{KD}$ Distillation loss, max iterations $T$

1. Initialize model parameters $\theta^{(0)}$ and $\lambda^0$.
2. for $t \in \{0, \ldots, T\}$ do
3. Update $\theta^{t+1}$ by Eq. 11.
4. if $t \% L == 0$ then
5. $x^{\text{train}}, y^{\text{train}} \leftarrow \text{SampleMiniBatch}(\mathcal{U})$
6. $x^{\text{val}}, y^{\text{val}} \leftarrow \text{SampleMiniBatch}(\mathcal{V})$
7. Compute one step update for model parameters as function of $\lambda^\lfloor t/L \rfloor$ by Eq.(7).
8. Update $\lambda^\lfloor t/L \rfloor+1$ by Eq.(10).
9. end if
10. end for

4 ALM-KD: Adaptive-Loss Mixing for KD

We formally define the optimization problem before outlining our ALM-KD algorithm for solving it. We propose to learn a student model that minimizes the following loss:

$$
L_{\text{student}}(\theta, \lambda) = \sum_i (1 - \lambda_i) L_s(y_i, x_i; \theta) + \lambda_i L_{KD}(y^{(S)}_i, y^{(T)}_i)
$$

(5)

This is a generalization of Eq. (3), with an instance-specific value of mixing parameter $\lambda_i$ corresponding to the $i^{th}$ training instance $x_i$. Jointly optimizing the objective in Eq.(5) with respect to both sets of parameters $\theta, \lambda$ on the training dataset alone can lead to severe overfitting. To mitigate this risk, we instead use a meta-learning procedure where we attempt to solve the following bi-level minimization problem.

$$
\underbrace{\argmin_{\lambda} L_{KD}(\underbrace{\argmin_{\theta} L_{\text{student}}(\theta, \lambda), \mathcal{V}}_{\text{inner-level}})}_{\text{outer-level}}
$$

(6)

By solving the inner level minimization, we wish to obtain model parameters $\theta$ that minimise the objective in Eq. (5). The outer minimization yields $\lambda$s such that the KL-divergence based loss in Eq.(2) is minimised on the validation set $\mathcal{V}$, with two major changes:
1) we set the temperature to $\tau = 1$
2) the target for distillation is the perturbed teacher’s output probability on the validation set $\mathcal{V}$.

For $(x_v, y_v) \in \mathcal{V}$, such newer targets can be derived as $p_{\alpha}^{T}(x_v) = (1 - \alpha)p^{T}(x_v) + \alpha e_{y_v}$, where $e_{y_v}$ is the corresponding one-hot encoding.

Note that $\alpha$ is a hyper parameter that controls the level of perturbation. Minimization of the KL-divergence based loss is intended to yield $\lambda$s that lead to loss mixing such that “dark knowledge” from the teacher is learnt. On the other hand, perturbation with one hot encoding ensures some robustness to spurious signals from an overfit teacher.\(^\dagger\)

\(^\dagger\)We can view $\alpha$ as a bootstrapping choice, since the “true” validation loss would itself involve some hypothetically optimal mixing values, and $\lambda$ for the validation data that are inaccessible during training.
Clearly, Eq.(6) is a bi-level optimisation problem. Since the inner optimisation problem cannot be solved in a closed form, we need to make some approximations in order to solve the optimization problem efficiently. We take an iterative approach, simultaneously updating the optimal model parameters and appropriate $\lambda$s in alternating steps as depicted in Figure 1. We first update the model parameters by sampling a mini-batch with $n$ instances from the training set, and simulating a one step look-ahead SGD update for the loss in Eq.(5) on model parameters ($\theta^t$) as a function of $\lambda^t$, resulting in Eq.(7).

$$\theta^{t+1} \left( \lambda^{|\ell|} \right) = \theta^t - \frac{\eta}{n} \sum_{i=1}^{n} \nabla_{\theta^t} \mathcal{L}_{\text{student}}(\theta^t, \lambda^{|\ell|}_i)$$

where $L$ is a hyperparameter governing how often the lambda values are updated. Using the approximate model parameters obtained using the one step look-ahead SGD update, the outer optimization problem is solved as,

$$\nabla_{\lambda^{|\ell|}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V}) = \nabla_{\theta^{t+1*}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V}), \nabla_{\lambda^{|\ell|}} \theta^{t+1*}$$

$$= -\frac{\eta}{n} \nabla_{\theta^{t+1*}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V}), \nabla_{\lambda^{|\ell|}} \nabla_{\theta^{t+1*}} \mathcal{L}_{\text{student}}$$

This can be re-written as,

$$\nabla_{\lambda^{|\ell|}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V}) =$$

$$= -\frac{\eta}{n} \nabla_{\theta^{t+1*}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V}), \nabla_{\lambda^{|\ell|}} [\nabla_{\theta^{t+1*}} \mathcal{L}_{KD} - \nabla_{\theta^{t+1*}} \mathcal{L}_{S_i}]^T$$

Here we perform a meta learning update to obtain the optimal $\lambda$ values to solve the outer optimisation problem.

Using the meta-gradient (in Eq.(8)), we update the $\lambda$s for each of the training samples using the first order gradient update rule (see Eq.(10)). Here, $\eta_{\lambda}$ is the learning rate for smoothing parameters across all classes.

$$\lambda^{|\ell|}_{i+1} = \lambda^{|\ell|}_i - \eta_{\lambda} \nabla_{\lambda^{|\ell|}} \mathcal{L}_{KD}(\theta^{t+1*}, \mathcal{V})$$
We update $\lambda$ values every $L$ epochs. The updated $\lambda_{i}^{[\frac{t}{L}] + 1}$ values are then used to update the model parameters as shown in Eq.(11).

$$\theta^{t+1} = \theta^{t} - \frac{\eta}{n} \sum_{i=1}^{n} \nabla_{\theta} L_{\text{student}}(\theta^{t}, \lambda_{i}^{[\frac{t}{L}]}$$

(11)

This algorithm for learning $\lambda$s via meta learning is presented in Algorithm 1. Whereas the positioning of this meta learning algorithm in the overall iterative scheme for Adaptive-Loss Mixing for KD (ALM-KD) is outlined in Figure 1.

### 4.1 Extending Meta Learning to multiple teachers

In the case that we have access to $K$ teachers we will have $K$ different KL divergence losses to match each of the teachers’ predictions. Again, we perform adaptive mixing of losses to estimate the relevance of the ground truth and a teacher’s logit for each of the point in the training set. Therefore we will have $\lambda$ controlling the influence of KL divergence loss associated with each of teacher. Thus, we can extend the loss in Eq.(3) as

$$L_{\text{multi}} = \sum_{i=1}^{n} (1 - \lambda_{\text{max},i}) L_{s}(x_{i}) + \left( \sum_{k=1}^{K} \lambda_{k,i} L_{KD_{k}}(x_{i}) \right)$$

(12)

where $\lambda_{\text{max},i} = \max(\lambda_{1,i}, \lambda_{2,i}, ..., \lambda_{n,i})$ is the maximum $\lambda_{k,i}$ value across all the $n$ teachers for the $i^{th}$ data point. Since each of the $\lambda_{k,i}$ weights the usefulness of the KL divergence loss with a $k^{th}$ teacher’s output as against the ground truth label for the $i^{th}$ data instance, in Eq.(12), we weigh the cross-entropy based loss associated with ground truth labels using $(1 - \lambda_{\text{max},i})$.

This yields another bi-level optimisation, analogous to Eq.(6)

$$\begin{align*}
\text{argmin}_{\lambda_{1}, \lambda_{2}, ..., \lambda_{K}} & \text{ argmin}_{\theta} L_{KD}(\theta, \lambda_{1}, \lambda_{2}, ..., \lambda_{K}, V) \\
\text{outer-level} & \text{inner-level}
\end{align*}$$

(13)

We perform a one step look-ahead SGD update analogous to Eq. 7 by replacing $L_{\text{student}}$ with $L_{\text{multi}}$, as

$$\theta^{t+1}(\lambda_{1}^{[\frac{t}{L}], 2}^{[\frac{t}{L}], ..., \lambda_{K}^{[\frac{t}{L}],}}) = \theta^{t} - \frac{\eta}{n} \sum_{i=1}^{n} \nabla_{\theta} \text{L}_{\text{student}}(\theta^{t}, \lambda_{1}^{[\frac{t}{L}],}, \lambda_{2}^{[\frac{t}{L}],}, ..., \lambda_{K}^{[\frac{t}{L}],})$$

Then for $\lambda_{k}$, the meta-gradient can be defined as,

$$\nabla_{\lambda_{k}} L_{KD}(\theta^{t+1}, V) = -\frac{\eta}{n} \nabla_{\theta} \text{L}_{KD}(\theta^{t+1}, V) \cdot \left[ \nabla_{\theta} \text{L}_{KD_{k}} - \nabla_{\theta} \text{L}_{s} \right]^{T}$$

(14)

$$\lambda_{k}^{[\frac{t}{L}] + 1} = \lambda_{k}^{[\frac{t}{L}],} - \eta \nabla_{\lambda_{k}} L_{KD}(\theta^{t+1}, V)$$

(15)

Similarly we can define meta-gradients to update $\lambda$s for the KL-divergence loss components associated with each of the other teacher models.

**Distilling with early stopped teachers** The loss presented in Eq.(12) is applicable to knowledge distillation from multiple teachers. We can also adapt it to knowledge distillation from an early stopped teacher as presented in (Cho & Hariharan, 2019), by simply gathering multiple teacher checkpoints, and using them together as multiple teachers in knowledge distillation. We discuss the results and implication of this approach in Section 6.3.
4.2 Implementation Details

We use the PyTorch (Paszke et al., 2017) framework to implement our algorithms. The main hyperparameters of the meta learning algorithm introduced in the previous section are $L$ and $\alpha$. In all our experiments we set $L = 10$ and $\alpha = 0.2$. Since the validation set is usually small, optimising $\lambda$s only on the validation set might cause $\lambda$ values to focus on minimising only the validation set. We prevent this by adding a training component to the objective as

$$\min_{\lambda} L_{KD}(\theta, V) + \beta L_{KD}(\theta, D)$$

We set $\beta = 0.1$ throughout our experiment. Implementing the one step look-ahead SGD update in Eq.(7) for modern deep models can be quite challenging and inefficient, especially since storing instance-wise gradients in the memory would be difficult. To tackle this problem, we adopt a last-layer gradient approximation similar to (Mirzasoleiman et al., 2020; Killamsetty et al., 2021b,a) by only considering the last layer gradients for neural networks.

5 Analysis of ALM-KD using synthetic data

We explore the performance and characteristics of our approach in synthetic data settings, to derive insight into the mechanisms by which ALM-KD can exploit instance-specific mixing parameters to improve upon state-of-the-art (SOTA) knowledge distillation models.

**Synthetic data generation:** We use the standard sklearn.datasets package (Pedregosa et al., 2011) to generate synthetic data with 14 features and 20 classes. The generated data has 8100 training points, 900 points in validation set and 1000 points in the test set. We randomly flip labels of 10% of the training data points to introduce noise. In Figure 7 in the Appendix, we provide a representative t-sne plot for an instance of synthetic data.

**Model architecture and experimental setup:** Knowledge distillation was performed on 2-layer neural network with 50 hidden nodes with 2-layer neural network with 80 hidden nodes as the teacher. Training consisted of SGD optimization with an initial learning rate of 0.01, momentum of 0.9, and weight decay of 5e-4. We trained for a total of 100 epochs using cosine annealing as the learning rate schedule.

5.1 $\lambda$s can counter label noise

Through this experimental setup, we examine the relationship between the teacher confidence, the label noise, and the learned $\lambda$ values of data points. We grouped training data points into buckets, based on the probability assigned by the teacher to its ground-truth label, and computed the average learned $\lambda$ per bucket; this averaging process was done separately for the instances with and without injected label noise. Finally, the experiment was repeated with 50 random seeds, and the averages as well as standard error of the mean (SEM) bars across those 50 runs are presented in Figure 3. We see two emerging patterns: Firstly, that as expected, the teacher assigns overall lower probabilities to the noisy labels in comparison to the other data points. Secondly, we see a trend wherein $\lambda$s learned for noisy labels are overall higher than for clean labels. This is because the meta-learning process learns that the ground-truth labels on those data points contribute poorly to generalization on the validation data, whereas, for such instances, the teacher probability is more informative than the ground-truth label. In Figure 8 in the Appendix, we also show that at model convergence (as expected), noisy labels have low teacher probabilities corresponding to the ground truth labels.
Figure 3: Relationship between teacher confidence, label noise, and learned $\lambda$s with mean and SEM error bars over 15 runs. As elaborated in Section 5.1, the teacher assigns relatively lower probabilities to noisy labels, and the meta-learning process in ALM-KD assigns higher $\lambda$ to noisy data points.

Figure 4: Learning trajectories: The figure shows generalization of test set accuracies (along with SEM bars) for vanilla KD, label-trained model, and ALM-KD, as a function of training epochs. All curves are averages over 50 runs.

5.2 Adaptive mixing and generalization

In a second experiment, we further examined the contributions of the meta-learning procedure to test-set generalization. In Figure 4, we present the test set accuracy as well as standard error of the mean (SEM) bars for various models as a function of training data epoch. Each curve is the average of 50 random synthetic data simulation-based training runs. We see that compared to the student model trained on the ground-truth data (i.e. the label-trained model), as well as the student trained with fixed $\lambda = 0.9$ (i.e. vanilla KD), ALM-KD learns faster, and converges to a higher test accuracy, driven by the adaptive loss mixing approach (c.f. Section 4).
Figure 5: Performance of ALM-KD across architectures and datasets, compared to two baselines with fixed loss mixing parameters $\lambda = \{0.1, 0.9\}$. Across a range of settings, ALM-KD is equivalent to, or better than, vanilla KD. For the experiments (a)-(c) we perform distillation on WRN-16-1 and in (d) we perform distillation on ResNet8.

6 Experiments on real-world datasets

We performed a range of experiments comparing ALM-KD against several SOTA knowledge distillation approaches on several real-world datasets.

Datasets The datasets in our experiments include CIFAR100 (Krizhevsky, 2009), CIFAR10 (Krizhevsky, 2009), Stanford Cars (Krause et al., 2013), Stanford Dogs (Khosla et al., 2011), and FGVC-Aircraft (Maji et al., 2013); characteristics of the datasets are summarized in Table 4 in the Appendix. For the CIFAR datasets we used the standard RGB images of size $32 \times 32$, whereas for the other datasets we used RGB images of size $224 \times 224$ which is the standard setting for FGVC-Aircraft, Stanford Cars and Dogs datasets.

Model architecture and experimental setup

We explored two families of models, viz., (i) Wide Residual Networks (WRN-16-1, WRN-16-3, WRN-16-4, WRN-16-6, WRN-16-8) (Zagoruyko & Komodakis, 2016), and (ii) ResNet (8, 14, 26, 32, 56) models (He et al., 2016) to show the effectiveness of our method across the different model families. We also perform a distillation on DenseNet 40-12 (Huang et al., 2016) with WRN-16-8 as a teacher model to show the effect of our technique in the cross-model distillation.

For datasets without pre-specified validation sets, we split the original training set into new train (90%) and validation sets (10%) (see Table 4 for details). Training consisted of SGD optimization with an initial learning rate of 0.1, momentum of 0.9, and weight decay of 5e-4. We divided the learning rate by 0.2 on epochs 60, 120 and 160 and trained for a total of 200 epochs.

6.1 Effect of optimal $\lambda$s on Knowledge Distillation

In the first experiment, we examine effective transfer of learned knowledge from various teachers to a student model which has fewer parameters. In Figures 5, we compare test accuracies obtained for vanilla KD (static $\lambda$s, $\lambda = 0.1$ curve in blue and $\lambda = 0.9$ curve in green) against ALM-KD (in red). KD with $\lambda = 0.1$ focuses primarily on cross entropy (Eq.(1)), and $\lambda = 0.9$ on teacher distillation.
| Dataset  | CIFAR-100 | Stanford Cars | Stanford Dogs |
|----------|------------|---------------|---------------|
| Method   |            |               |               |
| TAKD     | 67.29      | 45.10         | 50.33         |
| DGKD     | 68.61      | 48.45         | 51.36         |
| ALM-KD   | 67.8       | 50.87         | 51.44         |

Table 1: Multi-teacher setting: Teacher models WRN-16-3 and WRN-16-4 were used to perform distillation on the student model WRN-16-1. ALM-KD’s performance exceeds recent SOTA proposals for multi-teacher distillation.

(Eq.(2)). Here for a student model WRN-16-1 in Figures 5a-5c and for a student model ResNet-8 in Figure 5d we report performance across different teacher models. As seen in the figure, different teacher-student-dataset combinations work better with different $\lambda$ values, even in the vanilla KD setting. Our approach, ALM-KD, further improves upon these baselines by learning instance-specific mixing parameters. The gains of ALM-KD over baselines are consistent across experiments, with the exception of CIFAR100, for which the $\lambda = 0.9$ baseline performs comparably.

### 6.2 Knowledge Distillation with multiple teachers

The KD approach of transferring dark knowledge from large, complex teachers to simpler students sometimes fails when the gap between teacher & student representational capacities is very large. Recent approaches such as TAKD (Mirzadeh et al., 2019) and DGKD (Son et al., 2021) address this challenge: TAKD takes taking multiple KD training hops, with each step reducing the model complexity from teacher to student by a small amount. DGKD introduces all the intermediate teachers in a single KD training step and tries to optimise a loss similar to Eq.(15), although only using a single $\lambda$ per teacher. In addition, stochastic DGKD was proposed where a subset of teachers is introduced at each training step, determined by a binomial (hyperparameter) variable. This presents a need to control the contribution of each of the teachers in a systematic manner; therefore, we adapt our multi-teacher setting (Section 4.1) to learn optimal parameters for our training objective (Eq.(15)). We present results in Table 1, and observe that ALM-KD yields performance gains over both TAKD and DGKD. Teacher models WRN-16-3 and WRN-16-4 were used to perform distillation on the student model WRN-16-1. For both TAKD and DGKD we use $\lambda = 0.9$ and employ all teachers when evaluating DGKD.

### 6.3 Early Stopping and the multi-teacher setting

Another empirical approach to address the teacher-student representational gap is to simply stop teacher training at an intermediate stage, potentially simplifying the teacher signal (Cho & Hariharan, 2019). This approach raises a new challenge: how do we find an appropriate stopping point for the teacher, without having to train a large number of student models corresponding to teacher stopping points? We adapt our multi-teacher setting to solve this early stopping problem as follows: we train a single student model, with multiple teacher models, each stopped at intermediate points of the teacher training process. For this experiment, we trained a teacher model (WRN-16-8) on CIFAR-100 at the $20^{th}$, $70^{th}$, $130^{th}$ epochs as well as the final model, and trained two different student architectures viz. WRN-16-1 and DenseNet-40-12, using multi-teacher ALM-KD. In Table 2, we present the results; ALM-KD with early-stopped teachers consistently outperforms ALM-KD with only final model,
Table 2: Learning from early-stopped teacher: ALM-KD was trained with a range of teacher checkpoints (early stopping) in the multi-teacher setting. $\lambda$s obtained from ALM-KD’s meta learning process helps identify a good teacher, and exceed both vanilla KD and ALM-KD on the final teacher model alone. Here, the teacher model was WRN-16-8, and CIFAR-100 was used as dataset and also outperforms vanilla KD with a fixed $\lambda = 0.9$.

6.4 Early stopping: simplicity or overconfidence?

Figure 6 shows a very interesting result: as the teacher increased in confidence, the $\lambda$ values chosen by ALM-KD decreased ($\lambda$s are negative for confidence delta $> 0.2$), whereas if teacher confidence was largely unchanged, the $\lambda$ values were increased. This suggests that the primary challenge in the final teacher model is overfitting, with even noisy or ambiguous labels being confidently predicted by the teacher. Our validation-based objective, however, is able to identify those instances that the teacher is overconfident on (as they do not contribute to validation set accuracy), and able to downweight the teacher in those instances. Here again we grouped training data points into buckets,
Table 3: Self-distillation: Compared to traditional supervised learning (CE loss alone), both early stopping, and self-distillation show higher accuracy, as reported by earlier work. This shows that the model (WRN-16-8) overfits on the above datasets. We show that ALM-KD is easily applicable to the self-distillation setting, and provides additional gains in performance.

| Dataset → | FGVC-Aircraft | Stanford Dogs |
|-----------|---------------|---------------|
| Method ↓  |               |               |
| CE loss alone | 68.29        | 56.47         |
| Early stopped | 69.94        | 56.55         |
| CE loss     |               |               |
| Self-distillation | 71.17        | 58.17         |
| Self-distillation + ALM-KD | 72.53        | 58.42         |

Based on the probability assigned by the teacher to its ground-truth label, and computed the average learned $\lambda$ per bucket.

### 6.5 $\lambda$s for better generalisation

We now explore the self-distillation setting (Furlanello et al., 2018; Hahn & Choi, 2019), where the teacher and student models have identical architectures, and the goal is to train a student with better generalization accuracy than the teacher, through the use of the distillation loss for regularization. In Table 3, we present the results of our self-distillation experiment on the two datasets on which we found the teacher model (WRN-16-8) to be overfitting, viz., the FGVC-Aircraft and Stanford Dogs datasets. The first 3 rows reproduce known results; that on challenging datasets, both early stopping based on performance on validation set, and self-distillation, improve upon using CE loss alone. The final row shows that adaptive mixing via ALM-KD further improves upon self-distillation, thereby making it a potentially valuable tool in the traditional supervised learning setting in addition to teacher-student transfer for training smaller, more efficient student models.

### 7 Conclusion

Knowledge Distillation (KD) approaches have attempted to complement the ground-truth label information available in datasets with a label distribution obtained from a ‘teacher’ network against which the logits of a relatively simpler ‘student’ network can be matched. In this paper, we present an adaptive knowledge distillation scheme (ALM-KD) that titrates the teacher knowledge and ground truth label information through an instance-specific combination of teacher-matching and ground supervision objectives to learn student models that are more accurate than the teacher. Our iterative approach is pivoted on solving a bi-level optimization problem in which the instance weights are learnt to minimize the KD loss on a held-out validation set whereas the model parameters are themselves estimated to minimize the weight-combined ‘student’ network loss on the training dataset. Through synthetic experiments, we provide insights such as how the instance-specific parameters in ALM-KD can help counter label noise and can yield better generalization on test data. Through extensive experiments on real-world datasets, we present how ALM-KD yields accuracy improvement and better generalization on a range of datasets. The improvements hold even when ALM-KD is applied in conjunction with early stopped teacher models as well as with multiple teachers.
References

Algan, G. and Ulusoy, I. Meta soft label generation for noisy labels. In 2020 25th International Conference on Pattern Recognition (ICPR), pp. 7142–7148. IEEE, 2021.

Cho, J. H. and Hariharan, B. On the efficacy of knowledge distillation. In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 4794–4802, 2019.

Furlanello, T., Lipton, Z., Tschannen, M., Itti, L., and Anandkumar, A. Born again neural networks. In International Conference on Machine Learning, pp. 1607–1616. PMLR, 2018.

Gou, J., Yu, B., Maybank, S. J., and Tao, D. Knowledge distillation: A survey. International Journal of Computer Vision, 129(6):1789–1819, 2021.

Hahn, S. and Choi, H. Self-knowledge distillation in natural language processing. CoRR, abs/1908.01851, 2019. URL http://arxiv.org/abs/1908.01851.

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, pp. 770–778, 2016.

Heo, B., Lee, M., Yun, S., and Choi, J. Y. Knowledge distillation with adversarial samples supporting decision boundary. In Proceedings of the AAAI Conference on Artificial Intelligence, volume 33, pp. 3771–3778, 2019.

Hinton, G., Vinyals, O., and Dean, J. Distilling the knowledge in a neural network, 2015.

Huang, G., Liu, Z., and Weinberger, K. Q. Densely connected convolutional networks. CoRR, abs/1608.06993, 2016. URL http://arxiv.org/abs/1608.06993.

Khosla, A., Jayadevaprakash, N., Yao, B., and Fei-Fei, L. Novel dataset for fine-grained image categorization. In First Workshop on Fine-Grained Visual Categorization, IEEE Conference on Computer Vision and Pattern Recognition, Colorado Springs, CO, June 2011.

Killamsetty, K., Sivasubramanian, D., Ramakrishnan, G., De, A., and Iyer, R. Grad-match: Gradient matching based data subset selection for efficient deep model training. In International Conference on Machine Learning, 2021a.

Killamsetty, K., Sivasubramanian, D., Ramakrishnan, G., and Iyer, R. Glister: Generalization based data subset selection for efficient and robust learning. In AAAI, 2021b.

Krause, J., Stark, M., Deng, J., and Fei-Fei, L. 3d object representations for fine-grained categorization. In 4th International IEEE Workshop on 3D Representation and Recognition (3dRR-13), Sydney, Australia, 2013.

Krizhevsky, A. Learning multiple layers of features from tiny images. Technical report, 2009.

Liu, Y., Zhang, W., and Wang, J. Adaptive multi-teacher multi-level knowledge distillation. Neurocomputing, 415:106–113, 2020.

Maji, S., Kannala, J., Rahtu, E., Blaschko, M., and Vedaldi, A. Fine-grained visual classification of aircraft. Technical report, 2013.
Menon, A. K., Rawat, A. S., Reddi, S., Kim, S., and Kumar, S. A statistical perspective on distillation. In Meila, M. and Zhang, T. (eds.), *Proceedings of the 38th International Conference on Machine Learning*, volume 139 of *Proceedings of Machine Learning Research*, pp. 7632–7642. PMLR, 18–24 Jul 2021.

Mirzadeh, S.-I., Farajtabar, M., Li, A., Levine, N., Matsukawa, A., and Ghasemzadeh, H. Improved knowledge distillation via teacher assistant, 2019.

Mirzasoleiman, B., Bilmes, J., and Leskovec, J. Coresets for data-efficient training of machine learning models, 2020.

Paszke, A., Gross, S., Chintala, S., Chanan, G., Yang, E., DeVito, Z., Lin, Z., Desmaison, A., Antiga, L., and Lerer, A. Automatic differentiation in pytorch. In *NIPS-W*, 2017.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., and Duchesnay, E. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

Saxena, S., Tuzel, O., and DeCoste, D. Data parameters: A new family of parameters for learning a differentiable curriculum. *NeurIPS*, 2019.

Son, W., Na, J., Choi, J., and Hwang, W. Densely guided knowledge distillation using multiple teacher assistants, 2021.

Vyas, N., Saxena, S., and Voice, T. Learning soft labels via meta learning, 2020.

Wang, X., Zhang, R., Sun, Y., and Qi, J. Kdgan: Knowledge distillation with generative adversarial networks. In *NeurIPS*, pp. 783–794, 2018a.

Wang, Y., Xu, C., Xu, C., and Tao, D. Adversarial learning of portable student networks. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32, 2018b.

Wen, T., Lai, S., and Qian, X. Preparing lessons: Improve knowledge distillation with better supervision, 2020.

Zagoruyko, S. and Komodakis, N. Wide residual networks. In *BMVC*, 2016.

Zhao, H., Sun, X., Dong, J., Dong, Z., and Li, Q. Knowledge distillation via instance-level sequence learning. *Knowledge-Based Systems*, 233, 2021.

Zhou, T., Wang, S., and Bilmes, J. Robust curriculum learning: From clean label detection to noisy label self-correction. In *International Conference on Learning Representations*, 2020a.

Zhou, T., Wang, S., and Bilmes, J. A. Curriculum learning by dynamic instance hardness. *Advances in Neural Information Processing Systems*, 33, 2020b.
A Proof for Lemma

Statement: Assuming that the true label posterior is not known to the teacher, there exists an optimal $\lambda$ in Eq. (3), that leads to lower variance in the distilled risk.

**Proof:** Let $R_*$, $\hat{R}$ and $\tilde{R}$ denote the true risk associated with the oracle classifier $f$, empirical risk of the supervised student loss (Eq. 1) and teacher matching loss (Eq. 2), respectively. With this, Let $R$ denote the Risk obtained through the convex combination of both the losses (Eq. 3):

$$ R = \lambda \hat{R} + (1 - \lambda) \tilde{R} $$

Let $V()$ denote the variances of each of the Risk terms. We have,

$$ V(R) = V \left( \lambda \hat{R} + (1 - \lambda) \tilde{R} \right) $n$2 V(\hat{R}) + \lambda^2 V(\tilde{R}) + \lambda(1 - \lambda) \text{Cov}(\hat{R}, \tilde{R}) $$

$$ V(\hat{R}) = \frac{1}{N} \mathbb{E}_X \mathbb{E}_{y|X} \left[ l(y, f(x))^2 \right] 
- \frac{1}{N} \left[ \mathbb{E}_X \mathbb{E}_{y|X} (l(y, f(x))] \right]^2 
= \frac{1}{N} \mathbb{E}_X \mathbb{E}_{y|X} \left[ l(y, f(x))^2 \right] - \frac{1}{N} \tilde{R}_*^2 $$

$$ V(\tilde{R}) = \frac{1}{N} V \left[ \tilde{p}(x)^T l(f(x))] \right] 
= \frac{1}{N} V \left[ \mathbb{E}_{\tilde{Y}|X} l(y, f(x))] \right] 
= \frac{1}{N} \mathbb{E} \left[ \mathbb{E}_{\tilde{Y}|X} l(f(x))] \right]^2 
- \frac{1}{N} \left( \mathbb{E}_X \mathbb{E}_{y|X} l(y, f(x))] \right)^2 
= \frac{1}{N} \mathbb{E} \left[ \mathbb{E}_{\tilde{Y}|X} l(f(x))] \right]^2 - \frac{1}{N} \tilde{R}_*^2 $$

$$ \text{Cov}(\hat{R}, \tilde{R}) = \text{Cov}(\tilde{p}(x)^T l(f(x)), \tilde{p}(x)^T l(f(x))] 
= \text{Cov}(l(y, f(x)), \mathbb{E}_{\tilde{Y}|X} l(y, f(x))] 
= \mathbb{E} \left[ l(y, f(x))] \mathbb{E}_{\tilde{Y}|X} l(y, f(x))] \right] 
- \mathbb{E} l(y, f(x)) \mathbb{E} \mathbb{E}_{\tilde{Y}|X} l(y, f(x))] 
= \mathbb{E} \left[ l(y, f(x))] \mathbb{E}_{\tilde{Y}|X} l(y, f(x))] \right] - R_* \tilde{R}_* $$

Here, $p^t(x)$, $\tilde{p}(x)$ and $l$, respectively denote the true label posterior, teacher posterior and the loss functions. Note that $p^t(x) \neq \tilde{p}(x)$, implying that the teacher has not learned the correct label posterior.
Substituting Eq. 19, 20 and 21 in Eq. 18 -

\[
V(R) = \frac{\lambda^2}{N} E_{X \mid X} [(l(y, f(x))^2] - \frac{\lambda^2}{N} \tilde{R}_*^2 \\
+ \frac{(1 - \lambda)^2}{N} E_{X} \left[ E_{Y \mid X} l(y, f(x)) \right] - \frac{(1 - \lambda)^2}{N} \tilde{R}_*^2 \\
+ \lambda(1 - \lambda) E_{X,Y} \left[ l(y, f(x)) E_{Y \mid X} l(y, f(x)) \right] - R_* \tilde{R}_* \\
= \lambda^2 \left[ \frac{1}{N} (E_{X \mid Y} l^2 - \tilde{R}_*^2) \right] \\
+ (1 - \lambda)^2 \left[ \frac{1}{N} \left( E_{X,Y} (E_{Y \mid X} l)^2 - \tilde{R}_* \right) \right] \\
+ \lambda(1 - \lambda) \left[ E_{Y \mid X} l - R_* \tilde{R}_* \right] \\
= (a + b - c) \lambda^2 - (2b - c) \lambda + b
\] (22)

where,

\[
a = \frac{1}{N} (E_{X \mid Y} l^2 - \tilde{R}_*^2) \\
b = \frac{1}{N} \left( E_{X,Y} (E_{Y \mid X} l)^2 - \tilde{R}_* \right) \\
c = \left| E_{Y \mid X} l - R_* \tilde{R}_* \right|
\]

To get the optimal \(\lambda\), we differentiate Eq. 22 with respect to lambda and set the differential to zero. Therefore,

\[
\lambda^* = \frac{2b - c}{a + b - c}
\] (23)

Since, the Eq. 22 is quadratic in \(\lambda\), we have -

\[
V(\lambda^*) \leq V(\lambda) \quad \forall \lambda \\
\implies V(\lambda^*) \leq V(1) = V(\tilde{R}) \\
\implies V(\lambda^*) \leq V(0) = V(\tilde{R})
\] (24)

Thus, there exists an optimal \(\lambda\) (Eq. 23) that would lead to a the risk with lesser variance compared to individual terms. \(\Box\)

**B Synthetic experiments**

Figure 7 shows a t-sne projection of a synthetically generated dataset (generation details in the main body of the paper); as can be seen, the 20 classes have some spatial cohesiveness but also significant overlap, making it a nontrivial learning task to classify instances into their respective labels.

Figure 8 shows more details on the experiment presented in the main text (Figure 3); the right panel shows the distribution of converged teacher probabilities for noisy and clean labels, showing, as
expected, that the clean label data have a broad distribution of teacher probabilities for ground-truth label, with a right skew, whereas the noisy labels have a sharply leftward skew (i.e., very low teacher probabilities for ground-truth labels). This nicely complements the data in the left panel, showing that for noisy labels, and in general for less-confident teacher signals, the learned $\lambda$ values are higher, indicating that the teacher has more informative content (e.g., instance hardness, label ambiguity) than the ground-truth label in those scenarios.

C Dataset Details

Table 4 provides details of the various real-world datasets used in our experiments, and the partitioning of these datasets into train, validation (needed in our meta-learning procedure), and test data subsets. Wherever available, the existing splits provided by the source data were used; in other cases, 10% of the training data was partitioned off for use as validation data.

| Dataset            | #Classes | #Instances | #Train | #Validation | #Test  |
|--------------------|----------|------------|--------|-------------|--------|
| CIFAR100           | 100      | 60000      | 45000  | 5000        | 10000  |
| Stanford Cars      | 196      | 16185      | 7330   | 814         | 8,041  |
| Stanford Dogs      | 120      | 20580      | 10,800 | 1200        | 8,580  |
| FGVC-Aircraft      | 102      | 10200      | 6120   | 680         | 3400   |

Table 4: Number of classes, Number of instances in Train, Validation and Test splits in the different datasets

Figure 7: t-SNE plot of the synthetic data used.
Figure 8: Relationship between teacher confidence, label noise, and learned $\lambda$s.