# Friendly Sharpness-Aware Minimization <br> Supplementary Material 

## A1. Proof of Theorem 1

The proof is based on [4, 9]. We first introduce the Vector Bernstein inequality presented in [4].
Theorem $\mathbf{A 1}$ (Vector Bernstein). Let $\boldsymbol{x}_{1}, \ldots, \boldsymbol{x}_{\boldsymbol{n}}$ be independent, zero-mean vector-valued random variables with common dimension d. We have the waeker Vector Berstein version as follows

$$
\begin{equation*}
P\left(\left\|\sum_{i=1}^{n} \boldsymbol{x}_{\boldsymbol{i}}\right\| \geq \epsilon\right) \leq \exp \left(-\frac{\epsilon^{2}}{8 V}+\frac{1}{4}\right) \tag{1}
\end{equation*}
$$

where $V=\sum_{i=1}^{n} \mathbb{E}\left[\left\|\boldsymbol{x}_{\boldsymbol{i}}\right\|^{2}\right]$ is the sum of the variances of the centered vectors $\boldsymbol{x}_{\boldsymbol{i}}$.
Corollary A1. Let $\boldsymbol{x}_{\mathbf{1}}, \ldots, \boldsymbol{x}_{\boldsymbol{n}}$ be independent, zero-mean vector-valued random variables with common dimension $d$. Assume $\mathbb{E}\left[\left\|x_{i}\right\|^{2}\right] \leq M$. Let $w \in \Delta_{n}$ in the simplex. Then we have

$$
\begin{equation*}
P\left(\left\|\sum_{i=1}^{n} w_{i} \boldsymbol{x}_{\boldsymbol{i}}\right\| \geq \epsilon\right) \leq \exp \left(-\frac{\epsilon^{2}}{8 M\|w\|_{2}^{2}}+\frac{1}{4}\right) \tag{2}
\end{equation*}
$$

Proof. Simply apply Theorem A1 with $\hat{\boldsymbol{x}}_{\boldsymbol{i}}=w_{i} \boldsymbol{x}_{\boldsymbol{i}}$.
Now we can apply the above concentration results to prove Theorem 1.
Proof. First we separately bound the bias and variance, then use Corollary A1. The bias is:

$$
\begin{align*}
\left\|\sum_{t=1}^{T} w_{t} f\left(x_{t}\right)-f\left(x_{T}\right)\right\| & =\left\|\sum_{t=1}^{T} w_{t}\left(f\left(x_{t}\right)-f\left(x_{T}\right)\right)\right\|  \tag{3}\\
& \leq \sum_{t=1}^{T} w_{t}\left\|f\left(x_{t}\right)-f\left(x_{T}\right)\right\|  \tag{4}\\
& \leq \beta \sum_{t=1}^{T} w_{t}\left\|x_{t}-x_{T}\right\|  \tag{5}\\
& \leq \beta \sum_{t=1}^{T} w_{t} \sum_{s=t+1}^{T}\left\|x_{s}-x_{s-1}\right\|  \tag{6}\\
& \leq \gamma G \beta \sum_{t=1}^{T} w_{t}(T-t)  \tag{7}\\
& =\gamma G \beta \cdot \frac{1}{\sum_{t=1}^{T} \lambda^{T-t}} \cdot \sum_{t=1}^{T} \lambda^{T-t}(T-t) . \tag{8}
\end{align*}
$$

Note that by a well-known identity,

$$
\begin{equation*}
\sum_{t=1}^{T} \lambda^{T-t}(T-t)=\sum_{s=0}^{T-1} s \lambda^{s} \leq \sum_{s=0}^{\infty} s \lambda^{s}=\frac{\lambda}{(1-\lambda)^{2}} \tag{9}
\end{equation*}
$$

Hence, the bias is bounded by

$$
\begin{align*}
\gamma G \beta \cdot \frac{1}{\sum_{t=1}^{T} \lambda^{T-t}} \cdot \frac{\lambda}{(1-\lambda)^{2}} & =\gamma G \beta \cdot \frac{1-\lambda}{1-\lambda^{T}} \cdot \frac{\lambda}{(1-\lambda)^{2}}  \tag{10}\\
& =\gamma G \beta \cdot \frac{1}{1-\lambda^{T}} \cdot \frac{\lambda}{1-\lambda}  \tag{11}\\
& \leq G \beta \cdot \frac{\gamma}{(1-\lambda)\left(1-\lambda^{T}\right)} \tag{12}
\end{align*}
$$

Applying Corollary A1 to $x_{t}=x_{t}-f\left(x_{t}\right)$, we have that

$$
\begin{equation*}
\mathbb{P}\left(\left\|\sum_{t=1}^{T} w_{t}\left(y_{t}-f\left(x_{t}\right)\right)\right\|>k\right) \leq \exp \left(-\frac{\epsilon^{2}}{8 M^{2}\|w\|_{2}^{2}}+\frac{1}{4}\right) \tag{13}
\end{equation*}
$$

Now note that

$$
\begin{align*}
\|w\|_{2}^{2}=\sum_{t=1}^{T} w_{t}^{2} & =\frac{1}{\left(\sum_{t=1}^{T} \lambda^{T-t}\right)^{2}} \sum_{t=1}^{T}\left(\lambda^{2}\right)^{T-t}  \tag{14}\\
& =\frac{(1-\lambda)^{2}}{\left(1-\lambda^{T}\right)^{2}} \sum_{t=1}^{T}\left(\lambda^{2}\right)^{T-t}  \tag{15}\\
& =\frac{(1-\lambda)^{2}}{\left(1-\lambda^{T}\right)^{2}} \cdot \frac{1-\lambda^{2 T}}{1-\lambda^{2}}  \tag{16}\\
& =\frac{1-\lambda^{2 T}}{\left(1-\lambda^{T}\right)^{2}} \cdot \frac{(1-\lambda)^{2}}{1-\lambda^{2}}  \tag{17}\\
& =\frac{1+\lambda^{T}}{1-\lambda^{T}} \cdot \frac{1-\lambda}{1+\lambda}  \tag{18}\\
& \leq \frac{2(1-\lambda)}{1-\lambda^{T}} \tag{19}
\end{align*}
$$

Setting the right hand side of the high probability bound to $\delta$, we have concentration w.p. $1-\delta$ for $k$ satisfying

$$
\begin{equation*}
\delta \geq \exp \left(-\frac{\epsilon^{2}}{8 M\|w\|_{2}^{2}}+\frac{1}{4}\right) \tag{20}
\end{equation*}
$$

Rearranging, we find

$$
\begin{array}{r}
\log \left(e^{-\frac{1}{4}} / \delta\right) \leq \frac{\epsilon^{2}}{8 M\|w\|_{2}^{2}} \\
\Leftrightarrow \epsilon \geq 2 \sqrt{2} \sqrt{M}\|w\|_{2} \cdot \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)} \tag{22}
\end{array}
$$

Combining this with the triangle inequality,

$$
\begin{align*}
\left\|\sum_{t=1}^{T} w_{t} y_{t}-f\left(x_{T}\right)\right\| & \leq\left\|\sum_{t=1}^{T} w_{t} y_{t}-\sum_{t=1}^{T} w_{t} f\left(x_{t}\right)\right\|+\left\|\sum_{t=1}^{T} w_{t}\left(f\left(x_{t}\right)-f\left(x_{T}\right)\right)\right\|  \tag{23}\\
& \leq 2 \sqrt{2} \sqrt{M}\|w\|_{2} \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)}+G \beta \cdot \frac{\gamma}{(1-\lambda)\left(1-\lambda^{T}\right)}  \tag{24}\\
& \leq 2 \sqrt{2} \sqrt{\frac{2(1-\lambda)}{1-\lambda^{T}}} \sqrt{M} \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)}+G \beta \cdot \frac{\gamma}{(1-\lambda)\left(1-\lambda^{T}\right)}  \tag{25}\\
& \leq 4 \sqrt{M} \frac{\sqrt{1-\lambda}}{\sqrt{1-\lambda^{T}}} \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)}+G \beta \cdot \frac{\gamma}{(1-\lambda)\left(1-\lambda^{T}\right)} \tag{26}
\end{align*}
$$

with probability $1-\delta$. Since $1 / \sqrt{1-\lambda^{T}} \leq 1 /\left(1-\lambda^{T}\right)$, this can further be bounded by

$$
\begin{equation*}
\left(4 \sqrt{M} \cdot \sqrt{1-\lambda} \cdot \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)}+G \beta \cdot \frac{\gamma}{1-\lambda}\right) \cdot \frac{1}{1-\lambda^{T}} \tag{27}
\end{equation*}
$$

Write $\alpha=1-\lambda$. The inner part of the bound is optimized when

$$
\begin{align*}
4 \sqrt{M} \cdot \sqrt{\alpha} \cdot \sqrt{\log \left(e^{-\frac{1}{4}} / \delta\right)} & =G \beta \cdot \frac{\gamma}{\alpha}  \tag{28}\\
\Leftrightarrow \alpha^{3 / 2} & =\frac{G \beta \gamma}{4 \sqrt{M} \sqrt{\log \left(e^{\left.-\frac{1}{4} / \delta\right)}\right.}}  \tag{29}\\
\Leftrightarrow \alpha & =\frac{G^{2 / 3} \beta^{2 / 3} \gamma^{2 / 3}}{4^{2 / 3} \cdot M^{1 / 3} \cdot\left(\log \left(e^{-\frac{1}{4}} / \delta\right)\right)^{1 / 3}} \tag{30}
\end{align*}
$$

for which the overall inner bound is

$$
\begin{equation*}
2 G \beta \cdot \frac{\gamma}{\alpha}=2^{7 / 3} \cdot M^{1 / 3} \cdot \log \left(e^{-\frac{1}{4}} / \delta\right)^{1 / 3} \cdot(G \beta \gamma)^{1 / 3} \tag{31}
\end{equation*}
$$

If $T$ is sufficiently large, the $1 /\left(1-\lambda^{T}\right)$ term will be less than 2 . In particular,

$$
T>\frac{2}{\log (1+\alpha)} \Longrightarrow \frac{1}{1-(1-\alpha)^{T}}<2
$$

Since $\log (1+\alpha)>\alpha / 2$ for $\alpha<1$, it suffices to have $T>4 / \alpha$.

## A2. Proof of Lemma 1

## Proof.

$$
\begin{align*}
\mathbb{E}\left\langle\widetilde{\operatorname{Pro}}_{\nabla L\left(\boldsymbol{w}_{t}\right)}^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right), \nabla L\left(\boldsymbol{w}_{t}\right)\right\rangle & =\mathbb{E}\left\langle\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)-\sigma \boldsymbol{m}_{t}, \nabla L\left(\boldsymbol{w}_{t}\right)\right\rangle  \tag{32}\\
& =\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}(1-\sigma) . \tag{33}
\end{align*}
$$

Eqn. (33) uses the assumption that $\boldsymbol{m}_{t}$ is an unbiased estimator to $\nabla L\left(\boldsymbol{w}_{t}\right)$. Then with $\sigma=1$, we complete the proof.

## A3. Proof of Theorem 2

Proof. Denote $\boldsymbol{w}_{t+1 / 2}=\boldsymbol{w}_{t}+\rho \frac{\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)-\boldsymbol{m}_{t}}{\left\|\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)-\boldsymbol{m}_{t}\right\|}$. From Assumption 1, it follows that

$$
\begin{align*}
L\left(\boldsymbol{w}_{t+1}\right) \leq & L\left(\boldsymbol{w}_{t}\right)+\nabla L\left(\boldsymbol{w}_{t}\right)^{\top}\left(\boldsymbol{w}_{t+1}-\boldsymbol{w}_{t}\right)+\frac{\beta}{2}\left\|\boldsymbol{w}_{t+1}-\boldsymbol{w}_{t}\right\|^{2}  \tag{34}\\
= & L\left(\boldsymbol{w}_{t}\right)-\gamma_{t} \nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)+\frac{\gamma_{t}^{2} \beta}{2}\left\|\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)\right\|^{2}  \tag{35}\\
= & L\left(\boldsymbol{w}_{t}\right)-\gamma_{t} \nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right) \\
& +\frac{\gamma_{t}^{2} \beta}{2}\left(\left\|\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}-\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+2 \nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)\right)  \tag{36}\\
= & L\left(\boldsymbol{w}_{t}\right)-\frac{\gamma_{t}^{2} \beta}{2}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\frac{\gamma_{t}^{2} \beta}{2}\left\|\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}-\left(1-\beta \gamma_{t}\right) \gamma_{t} \nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)  \tag{37}\\
\leq & L\left(\boldsymbol{w}_{t}\right)-\frac{\gamma_{t}^{2} \beta}{2}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\gamma_{t}^{2} \beta\left\|\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L\left(\boldsymbol{w}_{t+1 / 2}\right)\right\|^{2} \\
& +\gamma_{t}^{2} \beta\left\|\nabla L\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}-\left(1-\beta \gamma_{t}\right) \gamma_{t} \nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right) . \tag{38}
\end{align*}
$$

The last step using the fact that $\|a-b\|^{2} \leq 2\|a-c\|^{2}+2\|c-b\|^{2}$. Then taking the expectation on both sides gives:

$$
\begin{equation*}
\mathbb{E}\left[L\left(\boldsymbol{w}_{t+1}\right)\right] \leq \mathbb{E}\left[L\left(\boldsymbol{w}_{t}\right)\right]-\frac{\gamma_{t}^{2} \beta}{2} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\gamma_{t}^{2} \beta M+\rho_{t}^{2} \gamma_{t}^{2} \beta^{3}-\left(1-\beta \gamma_{t}\right) \gamma_{t} \mathbb{E}\left[\nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)\right] \tag{39}
\end{equation*}
$$

For the last term, we have:

$$
\begin{align*}
\mathbb{E}\left[\nabla L\left(\boldsymbol{w}_{t}\right)^{\top} \nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)\right] & =\mathbb{E}\left[\nabla L\left(\boldsymbol{w}_{t}\right)^{\top}\left(\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)+\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)\right)\right] \\
& =\mathbb{E}\left[\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}\right]+\mathcal{C} \tag{40}
\end{align*}
$$

where $\mathcal{C}=\mathbb{E}\left[\nabla L\left(\boldsymbol{w}_{t}\right)^{\top}\left(\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)\right)\right]$. Using the Cauchy-Schwarz inequality, we have

$$
\begin{align*}
\mathcal{C} & \leq \mathbb{E}\left[\frac{1}{2}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\frac{1}{2}\left\|\nabla L\left(\boldsymbol{w}_{t+1 / 2}\right)-\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}\right] \\
& \leq \frac{1}{2} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\frac{\rho_{t}^{2} \beta^{2}}{2} \tag{41}
\end{align*}
$$

Plugging Eqn. (40) and (41) into Eqn. (39), we obtain:

$$
\begin{align*}
\mathbb{E}\left[L\left(\boldsymbol{w}_{t+1}\right)\right] \leq & \mathbb{E}\left[L\left(\boldsymbol{w}_{t}\right)\right]-\frac{\gamma_{t}^{2} \beta}{2} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\gamma_{t}^{2} \beta M+\rho_{t}^{2} \gamma_{t}^{2} \beta^{3}-\left(1-\beta \gamma_{t}\right) \gamma_{t} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}  \tag{42}\\
& +\left(1-\beta \gamma_{t}\right) \gamma_{t}\left(\frac{1}{2} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\frac{\rho_{t}^{2} \beta^{2}}{2}\right)  \tag{43}\\
\leq & \mathbb{E}\left[L\left(\boldsymbol{w}_{t}\right)\right]-\frac{\gamma_{t}}{2} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2}+\gamma_{t}^{2} \beta M+\frac{1}{2} \gamma_{t} \rho_{t}^{2} \beta^{2}\left(1+\beta \gamma_{t}\right) . \tag{44}
\end{align*}
$$

Taking summation over $T$ iterations, we have:

$$
\begin{equation*}
\frac{\gamma_{0}}{2 \sqrt{T}} \sum_{t=1}^{T} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2} \leq \mathbb{E}\left[L\left(\boldsymbol{w}_{0}\right)\right]-\mathbb{E}\left[L\left(\boldsymbol{w}_{T}\right)\right]+\left(\beta M+\frac{1}{2} \rho_{0}^{2} \beta^{3}\right) \gamma_{0}^{2} \sum_{t=1}^{T} \frac{1}{T}+\frac{1}{2} \rho_{0}^{2} \beta^{2} \gamma_{0} \sum_{t=1}^{T} \frac{1}{t} \tag{45}
\end{equation*}
$$

This gives

$$
\begin{align*}
\frac{1}{T} \sum_{t=1}^{T} \mathbb{E}\left\|\nabla L\left(\boldsymbol{w}_{t}\right)\right\|^{2} & \leq \frac{2\left(\mathbb{E}\left[L\left(\boldsymbol{w}_{0}\right)\right]-\mathbb{E}\left[L\left(\boldsymbol{w}_{T}\right)\right]\right)}{\gamma_{0} \sqrt{T}}+\frac{2 \beta M \gamma_{0}+\rho_{0}^{2} \beta^{3} \gamma_{0}}{\sqrt{T}}+\frac{\rho_{0}^{2} \beta^{2} \log T}{\sqrt{T}}  \tag{46}\\
& \leq \frac{2\left(\mathbb{E}\left[L\left(\boldsymbol{w}_{0}\right)-L\left(\boldsymbol{w}^{*}\right)\right]\right)}{\gamma_{0} \sqrt{T}}+\frac{2 \beta M \gamma_{0}+\rho_{0}^{2} \beta^{3} \gamma_{0}}{\sqrt{T}}+\frac{\rho_{0}^{2} \beta^{2} \log T}{\sqrt{T}}  \tag{47}\\
& =\frac{2 \Delta}{\gamma_{0} \sqrt{T}}+\frac{\Theta}{\sqrt{T}}+\frac{\Pi \log T}{\sqrt{T}} \tag{48}
\end{align*}
$$

where $\boldsymbol{w}^{*}$ is the optimal solution, $\Delta=\mathbb{E}\left[L\left(\boldsymbol{w}_{0}\right)-L\left(\boldsymbol{w}^{*}\right)\right], \Theta=2 \beta M \gamma_{0}+\rho_{0}^{2} \beta^{3} \gamma_{0}$, and $\Pi=\rho_{0}^{2} \beta^{2}$.

## A4. Extension to SAM's variants

Since we only modify the perturbation of SAM, our modification can be straightforwardly extended into the SAM variants, such as ASAM [5] and FiserSAM [3]. For SAM variants, their min-max objectives can be written into a unified formulation:

$$
\begin{equation*}
\min _{\boldsymbol{w}} \max _{\left\|T_{w}^{-1} \boldsymbol{\epsilon}\right\| \leq \rho} L(\boldsymbol{w}+\boldsymbol{\epsilon}), \tag{49}
\end{equation*}
$$

where $T_{w}$ is a normalization operator, e.g., $T_{w}=\|\boldsymbol{w}\|$ for ASAM. The inner maximization problem in Eq. (49) can then be solved via first-order approximation as follows:

$$
\begin{equation*}
\boldsymbol{\epsilon}_{s}=\rho \frac{T_{w}^{2} \nabla L_{\mathcal{B}}(\boldsymbol{w})}{\left\|T_{w} \nabla L_{\mathcal{B}}(\boldsymbol{w})\right\|_{2}} \tag{50}
\end{equation*}
$$

To incorporate our improvement, we can modify Eqn. (50) as follows:

$$
\begin{equation*}
\boldsymbol{\epsilon}_{s}=\rho \frac{T_{w}^{2}\left(\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)-\sigma \boldsymbol{m}_{t}\right)}{\left\|T_{w}\left(\nabla L_{\mathcal{B}}\left(\boldsymbol{w}_{t}\right)-\sigma \boldsymbol{m}_{t}\right)\right\|_{2}} \tag{51}
\end{equation*}
$$

VGG16-BN on CIFAR-100


Figure A1. Results on enlarging the batch size of SAM's adversarial perturbation.

## A5. Investigation Details

## A5.1. Experimental Settings

We follow the training setting of our main experiments.

Training from scratch. We train the models for 200 epochs and set the initial learning rate as 0.05 with a cosine learning rate schedule. The momentum and weight decay are set to 0.9 and 0.0005 for SGD, respectively. SAM adopt the same setting except that the weight decay is set to 0.001 following $[6,8]$. We apply standard random horizontal flipping, cropping, normalization, and cutout augmentation [1]. For SAM and its modified variants, we set the perturbation radius $\rho$ as 0.1 and 0.2 for CIFAR-10 and CIFAR-100 [6, 8].

Transfer learning. We use a Deit-small model [10] pre-trained on ImageNet. We use AdamW [7] as base optimizer and train the model for 10 epochs with batch size 128 , weight decay $10^{-5}$ and initial learning rate of $10^{-4}$. We adopt $\rho=0.075$ for SAM and its modified variants. We apply image resizing (to $224 \times 224$ ) and normalization for data preprocessing without extra augmentations.

SAM's modified variants. 1) SAM-full: we use full gradient $\nabla L(\boldsymbol{w})$ over the entire training dataset to calculate SAM's perturbation, i.e., $\boldsymbol{\epsilon}_{s}=\rho \frac{\nabla L(\boldsymbol{w})}{\|\nabla L(\boldsymbol{w})\|}$; 2) SAM-db: we use an extra random batch data $\mathcal{B}^{\prime}$ to calculate SAM's perturbation, i.e., $\boldsymbol{\epsilon}_{s}=\rho \frac{\nabla L_{\mathcal{B}^{\prime}}(\boldsymbol{w})}{\left\|\nabla L_{\mathcal{B}^{\prime}}(\boldsymbol{w})\right\|}$ 3) SAM-noise: we use residual projection direction w.r.t. the full gradient to calculate the perturbation, i.e., $\boldsymbol{\epsilon}_{s}=\rho \frac{\operatorname{Proj}_{\nabla L(\boldsymbol{w})}^{\top} \nabla L_{\mathcal{B}}(\boldsymbol{w})}{\left\|\operatorname{Proj}_{\nabla L(\boldsymbol{w})}^{\top} \nabla L_{\mathcal{B}}(\boldsymbol{w})\right\|}$. We align the gradient of the model parameters as a vector to perform gradient projection.

## A5.2. More Experiments on Effects of Full Gradient Component

To further substantiate the detrimental effects of strengthening the full gradient components, we conducted additional experiments on the CIFAR-100 dataset using the VGG16-BN architecture, as illustrated in Figure Fig. A1.

## A6. Training curves

In Fig. A2, we compare the training curves of SAM and F-SAM. We observe that F-SAM achieves a faster convergence than SAM especially on the initial stage. This is because at the initial stage, the proportion of the full gradient component in the minibatch gradient is more significant, and hence removing this component to facilitate convergence in F-SAM has a more pronounced effect. Moreover, as the perturbation radius grows ( 2 x in this case), the magnitude of the full gradient component
in $\boldsymbol{\epsilon}_{s}$ also grows. This can significantly hinder the convergence of SAM and degrade its performance. In contrast, F-SAM is able to mitigate this undesired effects and maintain a good performance.



Figure A2. Training curve comparison on CIFAR-100 with ResNet-18.

## A7. Hessian Spectrum

In Fig. A3, we compare the Hessian eigenvalues of ResNet-18 trained with SAM and F-SAM. We focus on the largest eigenvalue $\lambda_{1}$ and the ratio of the largest to the fifth largest eigenvalue $\lambda_{1} / \lambda_{5}$. We approximate the calculation for Hessian spectrum using the Lanczos algorithm [2]. We observe that F-SAM achieves a smaller largest eigenvalue and smaller eigenvalue ratio compared with SAM. This confirms that F-SAM converges to a flatter solution and achieves better generalization by removing the undesirable full gradient component in adversarial perturbation.


Figure A3. Hessian spectrum comparison on CIFAR-10 with ResNet-18.

## References

[1] Terrance DeVries and Graham W Taylor. Improved regularization of convolutional neural networks with cutout. arXiv preprint arXiv:1708.04552, 2017. 5
[2] Behrooz Ghorbani, Shankar Krishnan, and Ying Xiao. An investigation into neural net optimization via hessian eigenvalue density. In International Conference on Machine Learning, 2019. 6
[3] Minyoung Kim, Da Li, Shell X Hu, and Timothy Hospedales. Fisher sam: Information geometry and sharpness aware minimisation. In International Conference on Machine Learning (ICML), 2022. 4
[4] Jonas Moritz Kohler and Aurelien Lucchi. Sub-sampled cubic regularization for non-convex optimization. In International Conference on Machine Learning, pages 1895-1904. PMLR, 2017. 1
[5] Jungmin Kwon, Jeongseop Kim, Hyunseo Park, and In Kwon Choi. Asam: Adaptive sharpness-aware minimization for scaleinvariant learning of deep neural networks. In International Conference on Machine Learning (ICML), 2021. 4
[6] Bingcong Li and Georgios B Giannakis. Enhancing sharpness-aware optimization through variance suppression. arXiv preprint arXiv:2309.15639, 2023. 5
[7] Ilya Loshchilov and Frank Hutter. Decoupled weight decay regularization. arXiv preprint arXiv:1711.05101, 2017. 5
[8] Peng Mi, Li Shen, Tianhe Ren, Yiyi Zhou, Xiaoshuai Sun, Rongrong Ji, and Dacheng Tao. Make sharpness-aware minimization stronger: A sparsified perturbation approach. arXiv preprint arXiv:2210.05177, 2022. 5
[9] Matthew Staib, Sashank Reddi, Satyen Kale, Sanjiv Kumar, and Suvrit Sra. Escaping saddle points with adaptive gradient methods. In International Conference on Machine Learning (ICML), 2019. 1
[10] Hugo Touvron, Matthieu Cord, Matthijs Douze, Francisco Massa, Alexandre Sablayrolles, and Hervé Jégou. Training data-efficient image transformers \& distillation through attention. In International Conference on Machine Learning (ICML), 2021. 5

