CONSTRUCTING ORTHOGONAL CONVOLUTIONS IN AN EXPLICIT MANNER

Anonymous authors
Paper under double-blind review

ABSTRACT

The convolution with orthogonal input-output Jacobian matrix, *i.e.*, orthogonal convolution, has attracted substantial attention due to their excellent properties. A convolution layer with an orthogonal Jacobian matrix is 1-Lipschitz in the 2-norm, making the output robust to the perturbation in input. Meanwhile, an orthogonal Jacobian matrix preserves the gradient norm in back-propagation, which is critical for stable training deep networks. Nevertheless, existing orthogonal convolutions are burdened by high computational costs for preserving orthogonality. In this work, we exploit the relation between the singular values of the convolution layer's Jacobian and the structure of the convolution kernel. To achieve the orthogonality, we explicitly construct the convolution kernel for enforcing all singular values of the convolution layer's Jacobian to be 1s. After training, the explicitly constructed orthogonal (ECO) convolution can be constructed only once, and their weights are stored. Then, in evaluation, we only need to load the stored weights of the trained ECO convolution, and the computational cost of ECO convolution is the same as the standard dilated convolution. It is significantly more efficient than the recent state-of-the-art approach, skew orthogonal convolution (SOC) in evaluation. Our extensive experiments on CIFAR-10 and CIFAR-100 datasets demonstrate that the proposed ECO convolution is faster than SOC in evaluation while leading to competitive standard and certified robust accuracies.

1 INTRODUCTION

A layer with an orthogonal input-output Jacobian matrix is 1-Lipschitz in the 2-norm, robust to the perturbation in input. Meanwhile, it preserves the gradient norm in back-propagating the gradient, which effectively overcomes the gradient explosion and attenuation issues in training deep neural networks. In the past years, many studies have shown that exploiting orthogonality of the Jacobian matrix of layers in neural networks can achieve provable robustness to adversarial attacks (Li et al., 2019), stabler and faster training (Arjovsky et al., 2016; Xiao et al., 2018), and improved generalization (Cogswell et al., 2016; Bansal et al., 2018; Sedghi et al., 2019).

In a fully-connected layer $\mathbf{y} = \mathbf{W}\mathbf{x}$ where $\mathbf{W} \in \mathbb{R}^{c_{\text{out}} \times c_{\text{in}}}$ is the weight matrix, the layer's input-output Jacobian matrix $\mathbf{J} = \frac{\partial \mathbf{y}}{\partial \mathbf{x}}$ is just $\mathbf{W}$. Thus, preserving the orthogonality of $\mathbf{J}$ can be accomplished through imposing the orthogonal constraint on $\mathbf{W}$, which has been extensively studied in previous works (Mhammedi et al., 2017; Cissé et al., 2017; Anil et al., 2019). In contrast, in a convolution layer, the Jacobian matrix is no longer the weight matrix (convolution kernel). Instead, it is the circulant matrix composed of convolution kernel (Karami et al., 2019; Sedghi et al., 2019). Thus, generally, simply constructing an orthogonal convolution kernel cannot achieve an orthogonal convolution. Achieving an orthogonal Jacobian matrix in the convolution layer is more challenging than that in a fully-connected layer. It is plausibly straightforward to expand the convolution kernel to the doubly block circulant Jacobian matrix and directly impose the orthogonal constraint on the Jacobian matrix. Nevertheless, it is extremely difficult to construct a Jacobian matrix that is both doubly block-circulant and orthogonal.

Block Convolutional Orthogonal parameterization (BCOP) (Li et al., 2019) is one of the pioneering works for constructing the orthogonal convolution neural networks. It adopts the construction algorithm (Xiao et al., 2018) which decomposes a 2-D convolution into a stack of 1-D convolutions and a channel-wise orthogonal transformation. Trockman & Kolter (2021) maps the convolution kernel and the feature tensor into the frequency domain using Fast Fourier Transform (FFT), and achieves

the orthogonality of the Jacobian matrix through Cayley transform on the weight matrix in the frequency domain. They devise the convolution kernel of the same size as the input feature map, which takes more parameters than standard convolution layers with a local reception field. Meanwhile, FFT maps the real-value feature map and the weight matrix into matrices of complex values, increasing the computational cost to 4 times its counterpart in the real-value domain. Meanwhile, the Cayley transform requires computing the matrix inverse, which is not friendly for GPU computation. Recently, Skew Orthogonal Convolutions (SOC) (Singla & Feizi, 2021b) devises skew-symmetric filter and exploits matrix exponential (Hoogeboom et al., 2020) to attain the orthogonality of the Jacobian matrix. But SOC is slow in evaluation since it needs to apply a convolution filter multiple times sequentially on the feature map to obtain the Taylor expansion. Observing the efficiency limitations of the existing methods, in this work, we propose an explicitly constructed orthogonal (ECO) convolution, which is fast in both training and evaluation.

It is well known that the Jacobian matrix of a layer is orthogonal if and only if each of its singular values is 1. Thus we convert the problem of ensuring the orthogonality of the Jacobian matrix into making every singular value as 1. Based on the relation between the singular values of the Jacobian matrix for the convolution layer and the weight matrix of the convolution layer discovered by Sedghi et al. (2019), we construct the convolution kernel so that it ensures every singular value of the Jacobian matrix to be 1. Compared with the recent state-of-the-art method, SOC (Singla & Feizi, 2021b) implicitly approximating orthogonal convolution by multiple times convolution operations, ours explicitly builds the orthogonal convolution. Thus, we can directly deploy the constructed orthogonal convolution in evaluation, taking the same computational cost as the standard convolution. It is more efficient than SOC with multiple times convolution operations in evaluation. Experiments on CIFAR10 and CIFAR100 show that, in evaluation, taking less time, ours achieves competitive standard and robust accuracy compared with SOC.

2 Related Work

Weight orthogonalization. In a fully-connected layer, the input-output Jacobian matrix is the transform itself. Thus many efforts are devoted to orthogonalizing the weights. Some early works exploit an orthogonal weight initialization to speed up the training (Saxe et al., 2014; Pennington et al., 2017) and build extremely deep neural networks (Xiao et al., 2018). Recently, more efforts are devoted to exploiting the orthogonality not only in initialization but also in the whole training process. Some approaches propose "soft" constraints on the weight matrix. For example, Bansal et al. (2018); Xiong et al. (2016) introduce mutual coherence and spectral restricted isometry as orthogonal regularization on the weight matrix. Parseval Networks (Cissé et al., 2017) adapts a regularizer to encourage the orthogonality of the weight matrices. However, these methods can not guarantee the exact orthogonality of the weight matrix. Some approaches orthogonalize features during the forward pass. For example, Huang et al. (2018b) extends Batch Normalization (Ioffe & Szegedy, 2015) with ZCA; (Huang et al., 2018a) solves a suboptimization problem to decorrelate deep features. These methods can not avoid computationally expensive operations like SVD, thus slow in practice. Some approaches enforce orthogonality by using the Riemannian optimization on the Stiefel manifold. For example, Casado & Martínez-Rubio (2019) uses Pade approximation as an alternative to matrix exponential mapping to update the weight matrix on the Stifel manifold. Li et al. (2020) uses an iterative Cayley transform to enforce weight matrix orthonormal. Anil et al. (2019) also attains orthogonal weights by orthogonal parameterization based on Björck orthonormalization (BjoRick & Bowie, 1971). Lastly, some approaches incorporate orthogonal constraint into their network architecture. For example, Mhammedi et al. (2017) builds orthgonal layers in RNNs with householder reflections.

Orthogonal convolution. In a convolution layer, the Jacobian matrix is no longer the weight matrix. Thus, the above-mentioned weight orthogonalization methods cannot be trivially applied in convolution layers. Wang et al. (2020); Qi et al. (2020) encourage the orthogonality of the Jacobian matrix of convolution layers through a regularizer, but they cannot achieve the strict orthogonality and cannot attain the provable robustness. Block Convolutional Orthogonal parameterization (BCOP) (Li et al., 2019) is a pioneering work for enforcing the orthogonality of the Jacobian matrix of a convolution layer. It conducts parameterization of orthogonal convolutions by adapting the construction algorithm proposed by Xiao et al. (2018). But BCOP is slow in training. Trockman & Kolter (2021) applies the Cayley transform to a skew-symmetric convolution weight in the Fourier domain so that the convolution recovered from the Fourier domain has an orthogonal Jacobian matrix. Though it achieves higher efficiency in some applications than BCOP, it is still significantly more costly than

standard convolutional layers. Skew Orthogonal Convolution (Singla & Feizi, 2021b) achieves orthogonal convolution through Taylor expansion of the matrix exponential. It is faster than BCOP in training but slower in evaluation. In contrast, our method is efficient in both training and evaluation. Recently, Su et al. (2021) achieves orthogonal convolutions via paraunitary systems in an elegant manner. Nevertheless, it also suffers from inefficiency issue.

3 PRELIMINARY

Notation. For a matrix $\mathbf{M}$, $\mathbf{M}[i,j]$ denotes the element in the i-th row and the j-th column, $\mathbf{M}[i,:]$ denotes the i-th row and $\mathbf{M}[:,j]$ denotes the j-th column. We use the similar notation for indexing tensors. For $n \in \mathbb{N}$, $[n]$ denotes the set of n numbers from 0 to $n-1$, that is, $\{0, 1, \cdots, n-1\}$. We denote the function to obtain the singular values by $\sigma(\cdot)$. Let $\mathrm{vec}(\cdot)$ denotes the function which unfolds a matrix or higher-order tensor into a vector. Let $\omega_k = \exp(2\pi i/k)$ where $i = \sqrt{-1}$. Let $\mathbf{F}_k \in \mathbb{R}^{k\times k}$ be matrix for the discrete Fourier transform (DFT) for k-element vectors and each entry of $\mathbf{F}_k$ is defined as $\mathbf{F}_k[p,q] = \omega_k^{pq}$.

3.1 RELATION BETWEEN THE JACOBIAN MATRIX AND THE WEIGHT MATRIX

We denote the input tensor of a convolution layer by $\boldsymbol{\mathcal{X}} \in \mathbb{R}^{c\times n\times n}$, where n is the spatial size, and c is the number of input channels. We denote the convolution operation on $\boldsymbol{\mathcal{X}}$ by $\mathrm{conv}_{\hat{\boldsymbol{\mathcal{W}}}}(\boldsymbol{\mathcal{X}})$, where $\hat{\boldsymbol{\mathcal{W}}} \in \mathbb{R}^{k\times k\times c\times c}$ size where k is the size of the reception field and k is normally smaller than size of the input image, n. In this definition, we set the number of output channels identical to that of input channels. Meanwhile, we set the convolution stride as 1 and adapt the cyclic padding to make the output of the same size as the input.

We denote the output tensor by $\boldsymbol{\mathcal{Y}} \in \mathbb{R}^{c\times n\times n}$ and each element of $\boldsymbol{\mathcal{Y}}$ is obtained by

$$\forall l,s,t \in [c]\times[n]\times[n], \quad \boldsymbol{\mathcal{Y}}[l,s,t] = \sum_{r\in[c]}\sum_{p\in[k]}\sum_{q\in[k]} \boldsymbol{\mathcal{X}}[l+r, s+p, t+q]\hat{\boldsymbol{\mathcal{W}}}[p,q,l,r]. \tag{1}$$

Since the convolution operation is a linear transformation, there exists a linear transformation $\mathbf{M} \in \mathbb{R}^{n^2c\times n^2c}$ which satisfies:

$$\boldsymbol{\mathcal{Y}} = \mathrm{conv}_{\hat{\boldsymbol{\mathcal{W}}}}(\boldsymbol{\mathcal{X}}) \Leftrightarrow \mathrm{vec}(\boldsymbol{\mathcal{Y}}) = \mathbf{M}\mathrm{vec}(\boldsymbol{\mathcal{X}}). \tag{2}$$

To simplify illustration, $\hat{\boldsymbol{\mathcal{W}}} \in \mathbb{R}^{k\times k\times c\times c}$ is normally expanded into $\boldsymbol{\mathcal{W}} \in \mathbb{R}^{n\times n\times c\times c}$ through zero-padding. We term $\boldsymbol{\mathcal{W}}$ as the expanded convolution kernel. In $\boldsymbol{\mathcal{W}}$, only k^2c^2 elements are non-zero. Based on the above definition, we review the following theorem in Sedghi et al. (2019):

Theorem 1 (**see Sedghi et al. (2019) Section 2.2**)**.** *For any expanded convolution kernel $\boldsymbol{\mathcal{W}} \in \mathbb{R}^{n\times n\times c\times c}$, let $\mathbf{M}$ is the matrix encoding the linear transformation of a convolution with $\boldsymbol{\mathcal{W}}$. For each $p,q \in [n]\times[n]$, let $\mathbf{P}^{(p,q)}$ be the $c\times c$ matrix computed by*

$$\forall s,t \in [c]\times[c], \quad \mathbf{P}^{(p,q)}[s,t] = (\mathbf{F}_n^\top \boldsymbol{\mathcal{W}}[:,:,s,t]\mathbf{F}_n)[p,q]. \tag{3}$$

Then

$$\sigma(\mathbf{M}) = \bigcup_{p\in[n],q\in[n]} \sigma(\mathbf{P}^{(p,q)}). \tag{4}$$

The above theorem gives the relation between the singular values of the transformation matrix $\mathbf{M}$ and the expanded convolution $\boldsymbol{\mathcal{W}}$.

Theorem 2. *For any $\boldsymbol{\mathcal{W}} \in \mathbb{R}^{n\times n\times c\times c}$, the Jacobian matrix of the convolution layer, $\mathbf{J}$, is orthogonal if and only if $\forall p,q \in [n]\times[n]$, each singular value of the matrix $\mathbf{P}^{(p,q)}$ is 1.*

Proof. A real matrix is orthogonal if and only if each singular value is 1. Meanwhile, the Jacobian matrix $\mathbf{J} = \frac{\partial \mathrm{vec}(\boldsymbol{\mathcal{Y}})}{\partial \mathrm{vec}(\boldsymbol{\mathcal{X}})} = \mathbf{M}$. Based on Theorem 1, each singular value of $\mathbf{M}$ is 1 if and only if $\forall p,q \in [n]\times[n]$, each singular value of the matrix $\mathbf{P}^{(p,q)}$ is 1, thus we complete the proof.

3.2 MATRIX ORTHOGONALIZATION

Carley transform. Orthogonal parameterization has been extensively studied in the previous works. Many works (Absil et al., 2008; Helfrich et al., 2018; Maduranga et al., 2019) utilize Cayley transform on skew-symmetric matrices ($\mathbf{A}^\top$= -$\mathbf{A}$) to obtain the orthogonal weight matrices. Cayley

transform is a bijection between skew-symmetric matrices and orthogonal matrices without -1 eigenvalues. Specifically, it maps a skew-symmetric matrix $\mathbf{A}$ to an orthogonal matrix $\mathbf{Q}$ by

$$\mathbf{Q} = (\mathbf{I} - \mathbf{A})(\mathbf{I} + \mathbf{A})^{-1}. \tag{5}$$

Li et al. (2020) proposes an iterative approximation of the Cayley transform for orthogonally-constrained optimizers and achieves higher speed for training CNNs and RNNs.

Matrix exponential. Casado & Martínez-Rubio (2019) exploits the matrix exponential of the skew-symmetric matrix for orthogonal parameterization. To be specific, if $\mathbf{A}$ is a skew-symmetric matrix, $\exp(\mathbf{A})$ is orthogonal. Skew Orthogonal Convolutions (SOC) (Singla & Feizi, 2021b) approximates $\exp(\mathbf{A})$ through Taylor series $\exp(\mathbf{A}) \approx \mathbf{S}_T(\mathbf{A}) = \sum_{i=0}^{T} \frac{\mathbf{A}^i}{i!}$, and derives a bound on the approximation error:

$$\|\exp(\mathbf{A}) - \mathbf{S}_T(\mathbf{A})\|_2 \leq \frac{\|\mathbf{A}\|_2^T}{T!}, \tag{6}$$

where $\|\cdot\|_2$ denotes the spectral norm, which is the maximum singular value of a matrix. When $\|\mathbf{A}\|_2$ is small, the approximation can achieve high precision, thus SOC further adopts the spectral normalization on $\mathbf{A}$ to make $\|\mathbf{A}\|_2$ small.

Orthogonality of convolution. In a fully-connected layer, its Jacobian matrix is just the transpose of the weight matrix. Thus we can easily achieve the orthogonality of the Jacobian matrix through orthogonal parameterization on the weight matrix through the well-studied orthogonal parameterization approaches such as Cayley transform or matrix exponential of the skew-symmetric matrix. Nevertheless, in a convolution layer, the Jacobian matrix is no longer the transpose of the weight matrix. Thus we can not trivially apply the orthogonal parameterization approaches on the weight matrix to achieve the orthogonality of the Jacobian matrix.

3.3 Lipschitzness and Provably Robustness

Lipschitz constant. A function $f : \mathbb{R}^m \to \mathbb{R}^n$ is L-Lipschitz under the ℓ_2 norm iff $\|f(\mathbf{x}) - f(\mathbf{y})\|_2 \leq L\|\mathbf{x} - \mathbf{y}\|_2, \forall(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^m \times \mathbb{R}^m$, where L is a positive constant. We define the smallest value of L satisfying L-Lipschitz for f as the Lipschitz constant of f, denoted by $\mathrm{Lip}(f)$. Given two Lipschitz continuous functions f and g, the Lipschitz constant of the a composition of them, $\mathrm{Lip}(f \circ g)$, is upper-bounded by the product of the Lipschitz constants of f and g (Weaver, 2018):

$$\mathrm{Lip}(f \circ g) \leq \mathrm{Lip}(f)\mathrm{Lip}(g). \tag{7}$$

Thus, given a network $n(\cdot)$ consisting of L layers, if the Lipschitz constant of each layer is 1, the Lipschitz constant of the whole network, $\mathrm{Lip}(n)$ is less than 1.

Provably robustness. Considering a neural network $n(\cdot)$ for c-class classification. Given an input $\mathbf{x}$ with the ground-truth label $y \in [c]$, the network generates a c-dimensional prediction vector $n(\mathbf{x}) = [s_1, \cdots, s_c]$ where the i-th item in $n(\mathbf{x})$ denotes the confidence score for the class i. The margin of prediction for $\mathbf{x}$ by $n(\cdot)$ is defined as

$$\boldsymbol{\mathcal{M}}_n(\mathbf{x}) = \max(0, s_y - \max_{i \neq y} s_i). \tag{8}$$

As proved by Tsuzuku et al. (2018) and Li et al. (2019), for a network $n(\cdot)$ with a Lipschitz constant of L, $\mathbf{x}$ is provably robustly classified by $n(\cdot)$ under perturbation with a ℓ_2-norm of $\frac{\boldsymbol{\mathcal{M}}_n(\mathbf{x})}{\sqrt{2}L}$, that is,

$$\arg\max_i n(\mathbf{x} + \boldsymbol{\delta}) = y, \ \forall \|\boldsymbol{\delta}\|_2 < \frac{\boldsymbol{\mathcal{M}}_n(\mathbf{x})}{\sqrt{2}L}. \tag{9}$$

4 Method

Based on Theorem 2, to achieve an orthogonal Jacobian matrix $\mathbf{J}$ for a convolution layer, we need to ensure that, $\forall p, q \in [n] \times [n]$, each singular value of the matrix $\mathbf{P}^{(p,q)}$ is 1. When $\mathbf{P}^{(p,q)}$ is a real matrix, this condition is equivalent to the orthogonality of $\mathbf{P}^{(p,q)}$. To simplify the notation, we assemble the matrices $\mathbf{P}^{(p,q)}$ ($p, q \in [n] \times [n]$) into a tensor $\boldsymbol{\mathcal{P}} \in \mathbb{R}^{n \times n \times c \times c}$ such that $\boldsymbol{\mathcal{P}}[p, q, :, :] = \mathbf{P}^{(p,q)}$. Based on the definition, we rewrite the transformation from $\boldsymbol{\mathcal{W}}$ to $\mathbf{P}^{(p,q)}$ in Eq. (3) into

$$\forall s, t \in [c] \times [c], \boldsymbol{\mathcal{P}}[:, :, s, t] = \mathbf{F}_n^\top \boldsymbol{\mathcal{W}}[:, :, s, t]\mathbf{F}_n. \tag{10}$$

Since $\mathbf{F}_n$ is the full-rank square matrix, the mapping from $\boldsymbol{\mathcal{W}}$ to $\boldsymbol{\mathcal{P}}$ is invertible. Thus, to achieve an orthogonal Jacobian matrix, we can directly construct orthogonal $\boldsymbol{\mathcal{P}}[p, q, :, :]$ $(p, q \in [n] \times [n])$ using Carley transform or matrix exponential of skew-symmetric matrices (introduced in Section 3.2) to make each singular value of them identical to 1. Then the convolution kernel weight $\boldsymbol{\mathcal{W}}$ can be determined uniquely from the $\boldsymbol{\mathcal{P}}$ through the inverse transformation in Eq. (10). Since $\mathbf{F}_n$ is the Discrete Fourier Transform (DFT) matrix, $\mathbf{F}_n^\top \boldsymbol{\mathcal{W}}[:, :, s, t]\mathbf{F}_n$ in Eq. (10) is equivalent to conducting a 2-dimensional DFT on $\boldsymbol{\mathcal{W}}[:, :, s, t]$. Thus, we can recover $\boldsymbol{\mathcal{W}}[:, :, s, t]$ through the inverse 2-dimensional DFT (IDFT_{2D}) on the constructed orthogonal matrix $\boldsymbol{\mathcal{P}}[:, :, s, t]$. That is,

$$\boldsymbol{\mathcal{W}}[:, :, s, t] = \text{IDFT}_{\text{2D}}(\boldsymbol{\mathcal{P}}[:, :, s, t]), \quad \forall s, t \in [c] \times [c]. \tag{11}$$

Based on Theorem 2, the Jacobian matrix of the convolution layer with the kernel $\boldsymbol{\mathcal{W}}$ is orthogonal.

Nevertheless, the above approach has many drawbacks. First of all, for a generally constructed $\boldsymbol{\mathcal{P}}$, the recovered expanded convolution kernel $\boldsymbol{\mathcal{W}}$ computed based on the inverse 2-dimensional DFT might contain n^2c^2 non-zeros elements. It significantly increases the number of parameters in the convolution layer from k^2c^2 to n^2c^2. Meanwhile, the convolution with kernel $\boldsymbol{\mathcal{W}}$ has a global reception field, which is also slower than the original convolution kernel with a local reception field. Besides, the above approach needs to compute n^2 times matrix orthogonalization (Carley transform or matrix exponential) on $\boldsymbol{\mathcal{P}}[p, q, :, :]$ $(p, q \in [n] \times [n])$. Considering the spatial size of the input feature tensor, n and the input/out channel number c are not a small value, n^2 times orthogonalization on $c \times c$ matrices might be computationally expensive.

Thus, to achieve a high efficient orthogonal convolution, we devise a 2-dimensional periodic $\boldsymbol{\mathcal{P}}$. We set the period as k and assume n is divisible by k. Specifically, $\boldsymbol{\mathcal{P}}$ satisfies

$$\boldsymbol{\mathcal{P}}[p, q, :, :] = \boldsymbol{\mathcal{P}}[p + i * k, q + j * k, :, :], \quad \forall [p, q] \in [k] \times [k], [i, j] \in [n/k] \times [n/k]. \tag{12}$$

We define $\boldsymbol{\mathcal{P}}_0 = \boldsymbol{\mathcal{P}}[0{:}k, 0{:}k, :, :] \in \mathbb{R}^{k \times k \times c \times c}$. That is, $\boldsymbol{\mathcal{P}}$ can be obtained by repeating $\boldsymbol{\mathcal{P}}_0$ by $n/k \times n/k$ times in the first two dimensions. It has many benefits by the 2-dimensional periodic configuration. First of all, based on the property of DFT, the convolution kernel $\boldsymbol{\mathcal{W}}[:, :, s, t]$ obtained from an inverse 2D DFT on the 2-dimensional periodic $\boldsymbol{\mathcal{P}}[:, :, s, t]$ on contains only k^2 non-zero elements. That is, the number of non-zero elements in the recovered $\boldsymbol{\mathcal{W}}$ is only k^2c^2, which is the same as the number of elements in original convolution kernel $\hat{\boldsymbol{\mathcal{W}}}$ with a local reception field of $k \times k$ size. Besides, the non-zero elements in $\boldsymbol{\mathcal{W}}$ can be efficiently obtained. To be specific, we define $\boldsymbol{\mathcal{W}}_0 \in \mathbb{R}^{k \times k \times c \times c}$ obtained from $\boldsymbol{\mathcal{W}}_0[:, :, s, t] = \text{IDFT}_{\text{2D}}(\boldsymbol{\mathcal{P}}_0[:, :, s, t])$. Based on the property of DFT (Nussbaumer, 1981), $\boldsymbol{\mathcal{W}}$ and $\boldsymbol{\mathcal{W}}_0$ have the following relation:

$$\boldsymbol{\mathcal{W}}[i, j, :, :] = \begin{cases} \boldsymbol{\mathcal{W}}_0[\frac{i*k}{n}, \frac{j*k}{n}, :, :], & \text{if } i\%\frac{n}{k} = 0 \text{ and } j\%\frac{n}{k} = 0, \\ \mathbf{0}^{c \times c}, & \text{otherwise.} \end{cases} \tag{13}$$

That is, we can obtain the non-zero elements of $\boldsymbol{\mathcal{W}} \in \mathbb{R}^{n \times n}$ through computing $\boldsymbol{\mathcal{W}}_0 \in \mathbb{R}^{k \times k}$, which just takes only k^2 times 2D FFT on $c \times c$ matrices and is efficient. Moreover, since $\boldsymbol{\mathcal{P}}$ is periodic along the first two dimensions, to achieve an orthogonal Jacobian matrix based on Theorem 2, we only need to explicitly construct k^2 orthogonal matrices $\boldsymbol{\mathcal{P}}_0[p, q, :, :]$ $((p, q) \in [k] \times [k])$ to ensure that n^2 matrices $\boldsymbol{\mathcal{P}}[p, q, :, :]$ $((p, q) \in [n] \times [n])$ are orthogonal, which is also efficient. Moreover, as the recovered $\boldsymbol{\mathcal{W}}[i, j, :, :]$ is non-zero only if $i\%\frac{n}{k} = 0$ and $j\%\frac{n}{k} = 0$. This property corresponds to the dilated convolution (Yu & Koltun, 2016). Specifically, using the relation between $\boldsymbol{\mathcal{W}}$ and $\boldsymbol{\mathcal{W}}_0$ in Eq. (13), the following equation holds:

$$\text{Conv}_{\boldsymbol{\mathcal{W}}}(\boldsymbol{\mathcal{X}}) = \text{Conv}_{\boldsymbol{\mathcal{W}}_0}(\boldsymbol{\mathcal{X}}, \text{dilation} = \frac{n}{k}). \tag{14}$$

That is, we can achieve the orthogonal convolution through a dilated convolution with the kernel $\boldsymbol{\mathcal{W}}_0$ and the dilation n/k. The dilated convolution has been well supported by mainstream deep learning frameworks like Pytorch and Tensorflow. Based on above analysis, the process of achieving the orthogonal convolution is decomposed into three steps:

1. Construct the orthogonal matrices $\boldsymbol{\mathcal{P}}_0[p, q, :, :], \forall (p, q) \in [k] \times [k]$.
2. Recover $\boldsymbol{\mathcal{W}}_0[:, :, s, t]$ from $\boldsymbol{\mathcal{P}}_0[:, :, s, t]$ using inverse 2D DFT, $\forall (s, t) \in [c] \times [c]$.
3. Conduct the dilated convolution using the recovered kernel $\boldsymbol{\mathcal{W}}_0$ and the dilation n/k.

Algorithm 1: The proposed efficient orthogonal convolution. In training, the operations in lines 1-14 are involved in orthogonal convolution. In contrast, in evaluation, only the operation in line 14 is conducted, the operations in lines 1-13 have been conducted before evaluation and the obtained $\boldsymbol{\mathcal{W}}$ has been stored in the model for further evaluation.

Input: Input tensor $\boldsymbol{\mathcal{X}} \in \mathbb{R}^{n\times n\times c}$ where c is the number of input channels, the spatial size of the convolution, k, the parameter tensor $\hat{\boldsymbol{\mathcal{P}}}_0 \in \mathbb{R}^{L\times c\times c}$ (if k is odd, L is $\frac{k^2+1}{2}$ else $\frac{k^2+4}{2}$)

Output: Output tensor $\boldsymbol{\mathcal{Y}} \in \mathbb{R}^{n\times n\times c}$ from conducting orthogonal convolution on $\boldsymbol{\mathcal{X}}$.

1 **for** *all* $i \in [L]$ **do**
2 $\quad \hat{\boldsymbol{\mathcal{P}}}_0[i,:,:] \leftarrow \hat{\boldsymbol{\mathcal{P}}}_0[i,:,:] - \hat{\boldsymbol{\mathcal{P}}}_0[i,:,:]^\top$
3 $\quad \hat{\boldsymbol{\mathcal{P}}}_0[i,:,:] \leftarrow \mathrm{SpectralNorm}(\hat{\boldsymbol{\mathcal{P}}}_0[i,:,:])$
4 $\quad \hat{\boldsymbol{\mathcal{P}}}_0[i,:,:] \leftarrow \sum_{i=0}^{T} \frac{\hat{\boldsymbol{\mathcal{P}}}_0[i,:,:]^i}{i!}$
5 **end**
6 $\mathbf{I} = \mathrm{ConstructMap}(k)$ % construct the mapping matrix $\mathbf{I} \in \mathbb{R}^{k\times k}$
7 $\boldsymbol{\mathcal{P}}_0 = \mathrm{zeros}(k,k,c,c)$; $\boldsymbol{\mathcal{W}}_0 = \mathrm{zeros}(k,k,c,c)$
8 **for** *all* $(i,j) \in [k]\times[k]$ **do**
9 $\quad \boldsymbol{\mathcal{P}}_0[p,q,:,:] = \hat{\boldsymbol{\mathcal{P}}}_0[\mathbf{I}[p,q],:,:]$
10 **end**
11 **for** *all* $(s,t) \in [c]\times[c]$ **do**
12 $\quad \boldsymbol{\mathcal{W}}_0[:,:,s,t] = \mathrm{IDFT}_{2\mathrm{D}}(\boldsymbol{\mathcal{P}}_0[:,:,s,t])$
13 **end**
14 $\boldsymbol{\mathcal{Y}} = \mathrm{Conv}_{\boldsymbol{\mathcal{W}}_0}(\boldsymbol{\mathcal{X}}, \mathrm{dilation} = n/k)$
15 **return** $\boldsymbol{\mathcal{Y}}$

Below we introduce the details in these three steps individually.

Orthogonal parameterization for $\boldsymbol{\mathcal{P}}_0[p,q,:,:]$. This step can be implemented by any matrix orthogonalization approach such as Carley Transform on skew-symmetric matrix or matrix exponential of the skew-symmetric matrix. By default, we adopt the Taylor expansion for the exponential of the skew-symmetric matrix proposed in SOC (Singla & Feizi, 2021b) in this step considering its simplicity and efficiency. To be specific, we start from a parameter tensor $\boldsymbol{\mathcal{P}}_0 \in \mathbb{R}^{k\times k\times c\times c}$. $\forall\,(p,q) \in [k]\times[k]$, we compute

$$\begin{aligned}\boldsymbol{\mathcal{P}}_0[p,q,:,:] &\leftarrow \boldsymbol{\mathcal{P}}_0[p,q,:,:] - \boldsymbol{\mathcal{P}}_0[p,q,:,:]^\top,\\ \boldsymbol{\mathcal{P}}_0[p,q,:,:] &\leftarrow \sum_{i=0}^{T} \frac{\boldsymbol{\mathcal{P}}_0[p,q,:,:]^i}{i!}.\end{aligned} \tag{15}$$

Recall from Eq. (6) that the approximation error between $\exp(\mathbf{A})$ and the Taylor expansion $\mathbf{S}_k(\mathbf{A})$, $\|\exp(\mathbf{A}) - \mathbf{S}_k(\mathbf{A})\|_2$, is bounded by $\frac{\|A\|_2^k}{k!}$. That is, when $\|A\|_2 < 1$, it can achieve a good approximation. Thus, following SOC (Singla & Feizi, 2021b), we conduct spectral normalization on $\boldsymbol{\mathcal{P}}_0[p,q,:,:]$ so that $\|\exp(\mathbf{P}_0[p,q,:,:]) - \sum_{i=0}^{T} \frac{\boldsymbol{\mathcal{P}}_0[p,q,:,:]^i}{i!}\|_2 \leq \frac{\|\boldsymbol{\mathcal{P}}_0[p,q,:,:]\|_2^k}{k!} = \frac{1}{k!}$.

Recover $\boldsymbol{\mathcal{W}}_0$ from $\boldsymbol{\mathcal{P}}_0$. $\forall (s,t) \in [c]\times[c]$, inverse 2D DFT is on $\boldsymbol{\mathcal{P}}_0[:,:,s,t]$ to obtain $\boldsymbol{\mathcal{W}}_0[:,:,s,t]$:

$$\boldsymbol{\mathcal{W}}_0[:,:,s,t] = (\mathbf{F}_k^\top)^{-1}\boldsymbol{\mathcal{P}}_0[:,:,s,t]\mathbf{F}_k^{-1} = \mathrm{IDFT}_{2\mathrm{D}}(\boldsymbol{\mathcal{P}}_0[:,:,s,t]). \tag{16}$$

As $\boldsymbol{\mathcal{W}}_0$ is the convolution kernel for the further convolution, to make the convolution compatible with mainstream real-value convolutional neural networks, we should keep $\boldsymbol{\mathcal{W}}_0$ real. Based on the property of DFT, for inverse 2D discrete Fourier transform, the output $\mathbf{Y} \in \mathbb{R}^{k\times k}$ if purely real if and only if the input $\mathbf{X}$ is conjugate-symmetry, that is, $\mathbf{X}[i,j] = \mathbf{X}^*[(k-i)\%k, (k-j)\%k]$ for each $(i,j) \in [k]\times[k]$. Thus, to make $\boldsymbol{\mathcal{W}}_0$ real, we need set $\boldsymbol{\mathcal{P}}_0[i,j,:,:] := \boldsymbol{\mathcal{P}}_0^*[(k-i)\%k, (k-j)\%k, :,:]$ for each $(i,j) \in [k]\times[k]$. Since $\boldsymbol{\mathcal{P}}_0$ is real-value, we just need to set $\boldsymbol{\mathcal{P}}_0[i,j,:,:]$ and $\boldsymbol{\mathcal{P}}_0[(k-i)\%k, (k-j)\%k, :,:]$ identical. Due to the conjugate-symmetry settings, among these k^2 matrices $\{\boldsymbol{\mathcal{P}}_0[(i,j,:,:]\}_{i=1,j=1}^{k,k}$, there are only L different matrices. L is $(k^2+1)/2$ when k is odd and $(k^2+4)/2$ when k is even. In the implementation, we encode all the information of $\boldsymbol{\mathcal{P}}_0$ through a $L\times c\times c$ tensor $\hat{\boldsymbol{\mathcal{P}}}_0$. Then we build $\boldsymbol{\mathcal{P}}_0$ from $\hat{\boldsymbol{\mathcal{P}}}_0$ by a mapping matrix $\mathbf{I} \in \mathbb{R}^{k\times k}$:

$$\boldsymbol{\mathcal{P}}_0[i,j,:,:] = \hat{\boldsymbol{\mathcal{P}}}_0[\mathbf{I}[i,j],:,:], \forall (i,j) \in [k]\times[k], \tag{17}$$

where $\mathbf{I}$ is a mapping matrix, which maps a pair $(i, j) \in [k] \times [k]$ to a scalar $l \in [1, L]$ and it satisfies

$$\mathbf{I}[i, j] = \mathbf{I}[(k-i)\%k, (k-j)\%k], \forall (i, j) \in [k] \times [k]. \tag{18}$$

The details of constructing the mapping matrix $\mathbf{I}$ is provided in Algorithm 2 of Appendix A.

Dilation convolution. In this step, we conduct the standard dilated convolution using the recovered kernel $\boldsymbol{\mathcal{W}}_0$ obtained in Eq. (16) with a dilation n/k on the input $\boldsymbol{\mathcal{X}}$ and obtain the output $\boldsymbol{\mathcal{Y}}$.

We summarize the proposed model in Algorithm 1. It is worth noting that, in each training iteration, given a batch of B samples, the lines 1-13 are only conducted once, and the obtained $\mathcal{W}_0$ is shared across B samples. When the training finishes, we store the computed $\boldsymbol{\mathcal{W}}_0$ in line 12 in the model. In evaluation, we directly load the stored $\boldsymbol{\mathcal{W}}_0$ and only need to compute the operation in line 14, which is just vanilla dilated convolution and thus is very efficient.

In the current configuration of Algorithm 1, we set $\boldsymbol{\mathcal{P}}_0[p, q, :, :] \in \mathbb{R}^{c \times c}$ to be real matrix. In fact, $\boldsymbol{\mathcal{P}}_0[p, q, :, :]$ can also be complex matrix. To make the output of the proposed orthogonal convolution compatible with existing mainstream real-value neural network, the only constraint is to make $\boldsymbol{\mathcal{W}}_0[:, :, i, j] = \mathrm{IDFT}_{2\mathrm{D}}\boldsymbol{\mathcal{P}}_0[:, :, i, j]$ a real matrix. That is, the only constraint is to set $\boldsymbol{\mathcal{P}}_0[:, :, i, j]$ to be conjugate symmetric and thus $\boldsymbol{\mathcal{P}}_0[:, :, i, j]$ is unnecessarily real. When considering $\boldsymbol{\mathcal{P}}_0[p, q, :, :]$ as a complex matrix, it makes the constructed orthogonal convolution kernel $\boldsymbol{\mathcal{W}}_0$ more complete. Meanwhile, it brings more computational cost in training. In Appendix B, we compare with using a complex $\boldsymbol{\mathcal{P}}_0[p, q, :, :]$.

	Input Size	Output Size	Group 1		Group 2	
			Convolution	Repeats	Convolution	Repeats
Block 1	32×32	16×16	conv[3, 32, 1]	$(L/5 - 1)$	conv[3, 64, 2]	1
Block 2	16×16	8×8	conv[3, 64, 1]	$(L/5 - 1)$	conv[3, 128, 2]	1
Block 3	8×8	4×4	conv[3, 128, 1]	$(L/5 - 1)$	conv[3, 256, 2]	1
Block 4	4×4	2×2	conv[3, 256, 1]	$(L/5 - 1)$	conv[3, 512, 2]	1
Block 5	2×2	1×1	conv[3, 512, 1]	$(L/5 - 1)$	conv[3, 1024, 2]	1

Table 1: The configurations of the provably 1-Lipschitz architecture with L convolution layers. It consists of 5 blocks. Each block contains two groups of convolution layers. The first group contains $(L/5 - 1)$ convolution layers of stride 1, and the second group contains a single convolution layer of stride 2. The output size decreases to $1/2$ after each block. conv $[k, c, s]$ denotes the convolution with the kernel of spatial size $k \times k$, output channels c, stride s. The dilation of a convolution layer is $\lceil n/k \rceil$ where n is the spatial size of the input, and k is the spatial size of the convolution kernel.

5 Implementation

Spectral normalization. For a small approximation error from Taylor expansion, we conduct spectral normalization on $\mathbf{P}_0[p, q, :, :]$ to make $\|\mathbf{P}_0[p, q, :, :]\|_2 \leq 1$. Following Miyato et al. (2018); Singla & Feizi (2021a;b), we use the power method to estimate the approximated spectral norm and then divide $\mathbf{P}_0[p, q, :, :]$ by the estimated spectral norm. We use the mix-precision training supported by the APEX package for faster training and less GPU memory cost.

Padding. Following SOC (Singla & Feizi, 2021b), we use cyclic padding to substitute zero-padding since zero-padded orthogonal convolutions must be size 1 (see proof in Appendix D.2 of SOC (Singla & Feizi, 2021b)). To be specific, for a dilated convolution of $k \times k$ size with a dilation d, we add $d(k-1)/2$ paddings on each side in a cyclic manner.

Input and output channels. The proposed orthogonal convolution is devised under the condition that the number of channels in input is equal to that in output, that is, $c_{\text{in}} = c_{\text{out}} = c$. When $c_{\text{in}} \neq c_{\text{out}}$, following SOC (Singla & Feizi, 2021b), we additionally conduct the following operations:

1. if $c_{\text{in}} > c_{\text{out}}$, we apply our orthogonal convolution with a kernel size of $k \times k \times c_{\text{in}} \times c_{\text{in}}$, generating the output with c_{in} channels. We only select the first c_{out} channels in the output.
2. if $c_{\text{in}} < c_{\text{out}}$, we use zero pad the input with $c_{\text{out}} - c_{\text{in}}$ channels. Then we apply our orthogonal convolution with a kernel size of $k \times k \times c_{\text{out}} \times c_{\text{out}}$.

Strided convolution. Given an input $\boldsymbol{\mathcal{X}} \in \mathbb{R}^{n \times n \times c_{\text{in}}}$, a convolution with stride s generates the output $\mathcal{Y} \in \mathbb{R}^{\frac{n}{s} \times \frac{n}{s} \times c_{\text{out}}}$. The proposed orthogonal convolution is designed for 1-stride convolution.

For a more general s-stride convolution, we decompose it into a down-sampling module and an orthogonal convolution, following BCOP (Li et al., 2019) and SOC (Singla & Feizi, 2021b). Specifically, the down-sampling module adapts the invertible down-sampling (Maduranga et al., 2019), which simply reshapes the input feature map $\boldsymbol{\mathcal{X}}$ from $\mathbb{R}^{n\times n\times c_{\text{in}}}$ to $\mathbb{R}^{\frac{n}{s}\times\frac{n}{s}\times c_{\text{in}}s^2}$. The invertible down-sampling decreases the spatial size of the feature map from $k\times k$ to $k/s\times k/s$ and meanwhile strictly preserves the gradient norm. Then we conduct the proposed 1-stride orthogonal convolution on the reshaped $\boldsymbol{\mathcal{X}}$.

1-Lipschitz architecture. Following SOC (Singla & Feizi, 2021b), we build a provably 1-Lipschitz architecture based on the proposed orthogonal convolution. For a fair comparison with SOC, our structure is the same as SOC, and we only replace the orthogonal convolution in SOC with the proposed orthogonal convolution. The details of the architecture are given in Table 1. It consists of L convolution layers in 5 blocks, and each block contains $L/5$ layers. Each block consists of two groups of convolutions layers. The first group repeats $L/5-1$ convolutions layers with stride 1, and the second group contains a single convolution layer with stride 2, and the second group contains a single convolution layer with stride 2. Following SOC, a MaxMin activation function (Anil et al., 2019) is added after each convolution layer.

6 Experiments

Settings. The training is conducted on a single NVIDIA V100 GPU with 32G memory. Following Singla & Feizi (2021b), the whole training process takes 200 epochs for all models. The initial learning rate is 0.1 when the number of convolution layers is larger than 25 and 0.05 otherwise, and it decreases by a factor of 0.1 at the 50th and the 150th epoch. We set the weight decay as 0 when training BCOP (Li et al., 2019) and 5e-4 when training SOC (Singla & Feizi, 2021b) and our ECO. By default, we set the batch size as 256 on all models in training.

Evaluation metrics. We evaluate the performance proposed orthogonal convolution by two metrics: standard recognition accuracy and the robust recognition accuracy. The standard recognition

Model	Conv. Type	CIFAR10		CIFAR100		Time per Epoch (s)
		Standard Accuracy	Robust Accuracy	Standard Accuracy	Robust Accuracy	
LipConvnet-5	BCOP	74.35%	58.01%	42.61%	**28.67%**	40.4
	SOC	**75.78%**	**59.16%**	**42.73%**	27.82%	**16.1**
	ECO	73.38%	56.74%	41.81%	28.09%	26.3
LipConvnet-10	BCOP	74.47%	58.48%	42.08%	27.75%	59.1
	SOC	**76.48%**	**60.82%**	**43.71%**	29.39%	**26.3**
	ECO	73.64%	60.20%	41.85%	**30.22%**	37.1
LipConvnet-15	BCOP	73.86%	57.39%	39.98%	26.17%	79.5
	SOC	**76.88%**	61.30%	**42.93%**	28.79%	**36.5**
	ECO	74.72%	**63.99%**	41.80%	**30.92%**	50.4
LipConvnet-20	BCOP	69.84%	51.10%	36.13%	22.50%	100.7
	SOC	**76.43%**	61.92%	**43.07%**	29.18%	**43.5**
	ECO	75.42%	**64.65%**	41.45%	**32.25%**	63.2
LipConvnet-25	BCOP	68.26%	49.92%	28.41%	16.34%	123.5
	SOC	75.19%	60.18%	**43.31%**	28.59%	**53.1**
	ECO	**75.73%**	**66.14%**	41.66%	**32.59%**	75.7
LipConvnet-30	BCOP	64.11%	43.39%	26.87%	14.03%	145.2
	SOC	74.47%	59.04%	**42.90%**	28.74%	**62.5**
	ECO	**76.08%**	**67.19%**	39.46%	**29.49%**	89.4
LipConvnet-35	BCOP	63.05%	41.72%	21.71%	10.33%	170.1
	SOC	73.70%	58.44%	**42.22%**	28.31%	**72.4**
	ECO	**76.76%**	**67.45%**	39.41%	**31.34%**	115.5
LipConvnet-40	BCOP	60.17%	38.87%	19.97%	8.66%	188.3
	SOC	71.63%	54.36%	**41.83%**	27.98%	**80.8**
	ECO	**76.86%**	**67.84%**	40.43%	**30.98%**	114.3

Table 2: Comparisons among BCOP (Li et al., 2019), SOC (Singla & Feizi, 2021b) and our ECO convolution on standard accuracy, robust accuracy, the time cost per epoch in training.

accuracy is the same as that used in classic image classification. In contrast, the robust recognition accuracy is the accuracy under an l_2 perturbation. As shown in Section 3.3, L-Lipschitz network has the robustness certificate when the ℓ_2-norm perturbation ϵ is less than $\boldsymbol{\mathcal{M}}_n(\mathbf{x})/\sqrt{2}L$. Thus, for a 1-Lipschitz we built based on the proposed ECO convolution has the robustness certificate as $\boldsymbol{\mathcal{M}}_n(\mathbf{x})/\sqrt{2} \geq \epsilon$. Following Li et al. (2019) and Singla & Feizi (2021b), when testing the robust accuracy, we set the default norm of perturbation, ϵ, as $36/255$. In this case, the robust accuracy is the ratio of samples satisfying $\boldsymbol{\mathcal{M}}_n(\mathbf{x})/\sqrt{2} \geq 36/255$.

Standard and robust recognition accuracy. Table 2 compares the recognition accuracy of the proposed ECO convolution with BCOP (Li et al., 2019) and SOC (Singla & Feizi, 2021b) on CIFAR10 and CIFAR100 datasets. As we can observe from the table that our ECO convolution achieves competitive performance compared with BCOP and SOC in both standard and robust recognition accuracy. Specifically, on CIFAR-10 dataset, when the number of convolution layers, L, is larger than 25, ours outperforms both SOC and BCOP in standard and robust recognition accuracy. Meanwhile, on CIFAR-100 dataset, our ECO convolution achieves higher robust accuracy than SOC in all models from LipConvnet-5 to LipConvnet-40.

Model	LC-5	LC-10	LC-15	LC-20	LC-25	LC-30	LC-35	LC-40
SOC	1.827s	3.002s	4.140s	5.340s	6.520s	7.733s	8.680s	9.900s
ECO	**1.170**s	**1.191**s	**1.226**s	**1.322**s	**1.343**s	**1.410**s	**1.497**s	**1.573**s

Table 3: Comparisons between SOC (Singla & Feizi, 2021b) and our ECO convolution on the evaluation time for the testing split of CIFAR10 benchmark. LC denotes LipConvnet. In evaluation, we set the batch size as 128 and the evaluation is conducted on a single V100 GPU.

Training and evaluation time. As shown in the last column of Table 2, SOC is slightly more efficient than our ECO convolution in training. It is because the dilation convolution in our ECO adds more padding, making the input feature map larger than that in SOC. Meanwhile, as shown in Table 3, our ECO convolution is significantly faster than SOC in evaluation. It is due to that we have already constructed the ECO convolution before evaluation for once. Thus, in evaluation, the computational cost of our ECO convolution is the same as standard convolution. In contrast, SOC needs to take T times convolution operations per convolution layer to approximate the orthogonal convolution, which takes T times the computational cost as standard convolution. By default, SOC sets $T = 5$ in training and $T = 10$ in evaluation. As shown in Table 3, in LipConvnet-40, ours ECO convolution achieves an around $6\times$ speed-up ratio over SOC.

Robust accuracy with respect to distortion. As mentioned, the 1-Lipschitz network has the robustness certificate as $\boldsymbol{\mathcal{M}}_n(\mathbf{x})/\sqrt{2} \leq \epsilon$ and the testing accuracy is the ratio of samples satisfying $\boldsymbol{\mathcal{M}}_n(\mathbf{x})/\sqrt{2} \leq \epsilon$. We evaluate the robust accuracy of LipConvnet-25 when the distortion norm ϵ adapts different values. We compare with SOC and the robust accuracies of SOC under different ϵ are copied from Singla et al. (2021) using the same MaxMin activation function. As shown in Table 4, our ECO convolution consistently outperforms ECO under different ϵ and the advantage is more significant for a larger ϵ.

	CIFAR10			CIFAR100		
ϵ	$36/256$	$72/256$	$108/256$	$36/256$	$72/256$	$108/256$
SOC	60.17%	43.66%	28.60%	28.59%	18.18%	10.85%
ECO	**66.14**%	**55.57**%	**45.27**%	**32.59**%	**25.05**%	**19.19**%

Table 4: The robust accuracy with respect to the distortion norm ϵ.

7 Conclusion

This work investigates building the convolution layer with an orthogonal Jacobian matrix, which is 1-Lipschitz in the 2-norm and preserves the gradient. By exploiting the relation between the convolution kernel and the Jacobian matrix, we explicitly construct the convolution kernel to achieve the orthogonal convolution. The explicitly constructed orthogonal convolution (ECO) takes the exact computational cost as a standard dilated convolution in evaluation, which is more efficient than the existing state-of-the-art method, SOC, approximating the orthogonal convolution through multiple times convolution operations. Our experiments on CIFAR-10 and CIFAR-100 show that our ECO achieves competitive standard and robust accuracy as SOC using much less evaluation time.

REFERENCES

Pierre-Antoine Absil, Robert E. Mahony, and Rodolphe Sepulchre. *Optimization Algorithms on Matrix Manifolds*. Princeton University Press, 2008. ISBN 978-0-691-13298-3. URL http://press.princeton.edu/titles/8586.html.

Cem Anil, James Lucas, and Roger B. Grosse. Sorting out lipschitz function approximation. In Kamalika Chaudhuri and Ruslan Salakhutdinov (eds.), *Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA*, volume 97 of *Proceedings of Machine Learning Research*, pp. 291–301. PMLR, 2019. URL http://proceedings.mlr.press/v97/anil19a.html.

Martin Arjovsky, Amar Shah, and Yoshua Bengio. Unitary evolution recurrent neural networks. In *International Conference on Machine Learning*, pp. 1120–1128. PMLR, 2016.

Nitin Bansal, Xiaohan Chen, and Zhangyang Wang. Can we gain more from orthogonality regularizations in training deep cnns? In *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, pp. 4266–4276, 2018.

A. BjoRick and C. Bowie. An iterative algorithm for computing the best estimate of an orthogonal matrix. *Siam Journal on Numerical Analysis*, 8(2):358–364, 1971.

Mario Lezcano Casado and David Martínez-Rubio. Cheap orthogonal constraints in neural networks: A simple parametrization of the orthogonal and unitary group. In Kamalika Chaudhuri and Ruslan Salakhutdinov (eds.), *Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA*, volume 97 of *Proceedings of Machine Learning Research*, pp. 3794–3803. PMLR, 2019. URL http://proceedings.mlr.press/v97/lezcano-casado19a.html.

Moustapha Cissé, Piotr Bojanowski, Edouard Grave, Yann N. Dauphin, and Nicolas Usunier. Parseval networks: Improving robustness to adversarial examples. In Doina Precup and Yee Whye Teh (eds.), *Proceedings of the 34th International Conference on Machine Learning, ICML 2017, Sydney, NSW, Australia, 6-11 August 2017*, volume 70 of *Proceedings of Machine Learning Research*, pp. 854–863. PMLR, 2017. URL http://proceedings.mlr.press/v70/cisse17a.html.

Michael Cogswell, Faruk Ahmed, Ross B. Girshick, Larry Zitnick, and Dhruv Batra. Reducing overfitting in deep networks by decorrelating representations. In *4th International Conference on Learning Representations, ICLR 2016, San Juan, Puerto Rico, May 2-4, 2016, Conference Track Proceedings*, 2016.

Kyle Helfrich, Devin Willmott, and Qiang Ye. Orthogonal recurrent neural networks with scaled cayley transform. In Jennifer G. Dy and Andreas Krause (eds.), *Proceedings of the 35th International Conference on Machine Learning, ICML 2018, Stockholmsmässan, Stockholm, Sweden, July 10-15, 2018*, volume 80 of *Proceedings of Machine Learning Research*, pp. 1974–1983. PMLR, 2018. URL http://proceedings.mlr.press/v80/helfrich18a.html.

Emiel Hoogeboom, Victor Garcia Satorras, Jakub M. Tomczak, and Max Welling. The convolution exponential and generalized sylvester flows. In *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020, December 6-12, 2020, virtual*, 2020. URL https://proceedings.neurips.cc/paper/2020/hash/d3f06eef2ffac7faadbe3055a70682ac-Abstract.html.

Lei Huang, Xianglong Liu, Bo Lang, Adams Wei Yu, Yongliang Wang, and Bo Li. Orthogonal weight normalization: Solution to optimization over multiple dependent stiefel manifolds in deep neural networks. In *Thirty-Second AAAI Conference on Artificial Intelligence*, 2018a.

Lei Huang, Dawei Yang, Bo Lang, and Jia Deng. Decorrelated batch normalization. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 791–800, 2018b.

Sergey Ioffe and Christian Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. In *International conference on machine learning*, pp. 448–456. PMLR, 2015.

Mahdi Karami, Dale Schuurmans, Jascha Sohl-Dickstein, Laurent Dinh, and Daniel Duckworth. Invertible convolutional flow. 2019.

Jun Li, Fuxin Li, and Sinisa Todorovic. Efficient riemannian optimization on the stiefel manifold via the cayley transform. In *8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020*. OpenReview.net, 2020. URL https://openreview.net/forum?id=HJxV-ANKDH.

Qiyang Li, Saminul Haque, Cem Anil, James Lucas, Roger B Grosse, and Jörn-Henrik Jacobsen. Preventing gradient attenuation in lipschitz constrained convolutional networks. *Advances in neural information processing systems*, 32:15390–15402, 2019.

Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. *arXiv preprint arXiv:1706.06083*, 2017.

Kehelwala D. G. Maduranga, Kyle E. Helfrich, and Qiang Ye. Complex unitary recurrent neural networks using scaled cayley transform. In *The Thirty-Third AAAI Conference on Artificial Intelligence, AAAI 2019, The Thirty-First Innovative Applications of Artificial Intelligence Conference, IAAI 2019, The Ninth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2019, Honolulu, Hawaii, USA, January 27 - February 1, 2019*, pp. 4528–4535. AAAI Press, 2019. doi: 10.1609/aaai.v33i01.33014528. URL https://doi.org/10.1609/aaai.v33i01.33014528.

Zakaria Mhammedi, Andrew Hellicar, Ashfaqur Rahman, and James Bailey. Efficient orthogonal parametrisation of recurrent neural networks using householder reflections. In *International Conference on Machine Learning*, pp. 2401–2409. PMLR, 2017.

Takeru Miyato, Toshiki Kataoka, Masanori Koyama, and Yuichi Yoshida. Spectral normalization for generative adversarial networks. In *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*. OpenReview.net, 2018. URL https://openreview.net/forum?id=B1QRgziT-.

Henri J Nussbaumer. The fast fourier transform. In *Fast Fourier Transform and Convolution Algorithms*, pp. 80–111. Springer, 1981.

Jeffrey Pennington, Samuel S. Schoenholz, and Surya Ganguli. Resurrecting the sigmoid in deep learning through dynamical isometry: theory and practice. In Isabelle Guyon, Ulrike von Luxburg, Samy Bengio, Hanna M. Wallach, Rob Fergus, S. V. N. Vishwanathan, and Roman Garnett (eds.), *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, pp. 4785–4795, 2017. URL https://proceedings.neurips.cc/paper/2017/hash/d9fc0cdb67638d50f411432d0d41d0ba-Abstract.html.

Haozhi Qi, Chong You, Xiaolong Wang, Yi Ma, and Jitendra Malik. Deep isometric learning for visual recognition. In *International Conference on Machine Learning*, pp. 7824–7835. PMLR, 2020.

Andrew M. Saxe, James L. McClelland, and Surya Ganguli. Exact solutions to the nonlinear dynamics of learning in deep linear neural networks. In Yoshua Bengio and Yann LeCun (eds.), *2nd International Conference on Learning Representations, ICLR 2014, Banff, AB, Canada, April 14-16, 2014, Conference Track Proceedings*, 2014. URL http://arxiv.org/abs/1312.6120.

Hanie Sedghi, Vineet Gupta, and Philip M. Long. The singular values of convolutional layers. In *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*, 2019. URL https://openreview.net/forum?id=rJevYoA9Fm.

Sahil Singla and Soheil Feizi. Fantastic four: Differentiable and efficient bounds on singular values of convolution layers. In *9th International Conference on Learning Representations, ICLR 2021, Virtual Event, Austria, May 3-7, 2021*. OpenReview.net, 2021a. URL https://openreview.net/forum?id=JCRblSgs34Z.

Sahil Singla and Soheil Feizi. Skew orthogonal convolutions. In *Proceedings of the 38th International Conference on Machine Learning, ICML 2021, 18-24 July 2021, Virtual Event*, pp. 9756–9766, 2021b. URL http://proceedings.mlr.press/v139/singla21a.html.

Sahil Singla, Surbhi Singla, and Soheil Feizi. Householder activations for provable robustness against adversarial attacks. *CoRR*, abs/2108.04062, 2021. URL https://arxiv.org/abs/2108.04062.

Jiahao Su, Wonmin Byeon, and Furong Huang. Scaling-up diverse orthogonal convolutional networks with a paraunitary framework. *arXiv preprint arXiv:2106.09121*, 2021.

Asher Trockman and J. Zico Kolter. Orthogonalizing convolutional layers with the cayley transform. In *9th International Conference on Learning Representations, ICLR 2021, Virtual Event, Austria, May 3-7, 2021*, 2021. URL https://openreview.net/forum?id=Pbj8H_jEHYv.

Yusuke Tsuzuku, Issei Sato, and Masashi Sugiyama. Lipschitz-margin training: Scalable certification of perturbation invariance for deep neural networks. In Samy Bengio, Hanna M. Wallach, Hugo Larochelle, Kristen Grauman, Nicolò Cesa-Bianchi, and Roman Garnett (eds.), *Advances in Neural Information Processing Systems 31: Annual Conference on Neural Information Processing Systems 2018, NeurIPS 2018, December 3-8, 2018, Montréal, Canada*, pp. 6542–6551, 2018. URL https://proceedings.neurips.cc/paper/2018/hash/485843481a7edacbfce101ecb1e4d2a8-Abstract.html.

Jiayun Wang, Yubei Chen, Rudrasis Chakraborty, and Stella X Yu. Orthogonal convolutional neural networks. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 11505–11515, 2020.

Nik Weaver. *Lipschitz algebras*. World Scientific, 2018.

Lechao Xiao, Yasaman Bahri, Jascha Sohl-Dickstein, Samuel S. Schoenholz, and Jeffrey Pennington. Dynamical isometry and a mean field theory of cnns: How to train 10, 000-layer vanilla convolutional neural networks. In Jennifer G. Dy and Andreas Krause (eds.), *Proceedings of the 35th International Conference on Machine Learning, ICML 2018, Stockholmsmässan, Stockholm, Sweden, July 10-15, 2018*, volume 80 of *Proceedings of Machine Learning Research*, pp. 5389–5398. PMLR, 2018. URL http://proceedings.mlr.press/v80/xiao18a.html.

Wei Xiong, Bo Du, Lefei Zhang, Ruimin Hu, and Dacheng Tao. Regularizing deep convolutional neural networks with a structured decorrelation constraint. In *2016 IEEE 16th International Conference on Data Mining (ICDM)*, pp. 519–528. IEEE, 2016.

Fisher Yu and Vladlen Koltun. Multi-scale context aggregation by dilated convolutions. In Yoshua Bengio and Yann LeCun (eds.), *4th International Conference on Learning Representations, ICLR 2016, San Juan, Puerto Rico, May 2-4, 2016, Conference Track Proceedings*, 2016. URL http://arxiv.org/abs/1511.07122.

Algorithm 2: Constructing the mapping matrix $\mathbf{I}$

Input: The spatial size of the convolution kernel, k.
Output: The mapping matrix $\mathbf{I}$

```
I = zeros(k, k);
count = 0;
for all (i, j) ∈ [k] × [k] do
    if I[(k − i)%k, (k − j)%k] == 0 then
        I[i, j] = count;
        count = count + 1;
    end
    else
        I[i, j] = I[(k − i)%k, (k − j)%k];
    end
end
return I
```

A Constructing the mapping matrix $\mathbf{I}$

In Algorithm 2, we give the details of constructing the mapping matrix $\mathbf{I}$.

B Comparisons with the complex settings

As we mentioned in Section 4, to obtain a real-value convolution kernel $\boldsymbol{\mathcal{W}}_0$, the entries in $\boldsymbol{\mathcal{P}}_0$ are unnecessarily real. We compare the performance when $\boldsymbol{\mathcal{P}}_0$ is constrained to be real as Algorithm 1 and that when $\boldsymbol{\mathcal{P}}_0$ is a complex tensor. As shown in Table 5, on CIFAR-10 benchmark, using complex $\boldsymbol{\mathcal{P}}_0$, it consistently outperforms its real counterpart on both standard accuracy and robust accuracy. The accuracy gap between the complex $\boldsymbol{\mathcal{P}}_0$ and its real counterpart is large for shallow networks and turns smaller as the network goes deeper. It is worth noting that the computational cost of multiplication between complex matrices is four times as that between real matrices of the same sizes. But the complex $\boldsymbol{\mathcal{P}}_0$ is only used for constructing the real orthogonal kernel $\boldsymbol{\mathcal{W}}_0$. After kernel construction, the computation cost of convolution is the same for the layer with complex $\boldsymbol{\mathcal{P}}_0$ and that with real $\boldsymbol{\mathcal{P}}_0$. Thus, as shown in Table 5, the training time per epoch when using complex $\boldsymbol{\mathcal{P}}_0$ is around 2 to 3 times as that using real $\boldsymbol{\mathcal{P}}_0$. In evaluation, since we have constructed the real $\boldsymbol{\mathcal{W}}_0$ from a real or complex $\boldsymbol{\mathcal{P}}_0$ before evaluation, the computational cost is the same no matter $\boldsymbol{\mathcal{P}}_0$ is complex and real.

	Standard Accuracy		**Robust Accuracy**		**Training Time**	
Model	**LC-10**	**LC-15**	**LC-10**	**LC-15**	**LC-10**	**LC-15**
Real	73.64	60.20	74.72	63.99	**37.1**	**50.4**
Complex	**75.40**	**64.50**	**76.53**	**69.02**	100.5	117.3

Table 5: Comparisons between the real and complex $\boldsymbol{\mathcal{P}}_0$ on CIFAR-10 dataset. LC is the abbreviation for LipConvnet.

C Comparisons with the standard convolution

Here, we compare the proposed orthogonal convolution with the standard convolution without orthogonal constraint. To make a fair comparison, we only replace the orthogonal convolution layers of LipConvnet-5 by the standard convolution and keep the other layers unfixed. Since the network built upon the standard convolution cannot preserve the 1-Lipschitz property, we cannot directly obtain the robust accuracy based on $\boldsymbol{\mathcal{M}}_n(\mathbf{x})$ as the original LipConvnet-5 network. Thus, we utilize Projected Gradient Descent (PGD) attack (Madry et al., 2017) to obtain the robust accuracy upper bound under the distortion with the ℓ_2 norm less than $\frac{36}{255}$. The results are shown in Table 6. As shown in the table, on both CIFAR10 and CIFAR10 datasets, the network based on the standard con-

volution achieves higher standard accuracy than the network based on our ECO convolution. In the meanwhile, ours achieves higher robust accuracy on both datasets under the same scale of distortion.

	CIFAR10		CIFAR100	
	Standard Accuracy	**Robust Accuracy**	**Standard Accuracy**	**Robust Accuracy**
Standard	**77.34%**	11.85%	**48.89%**	8.27%
ECO	73.38%	**56.74%**	41.81%	**28.09%**

Table 6: Comparisons with the standard convolution.

D STANDARD TRAINING ON RESNET

We conduct experiments based on the ResNet-18, which is one of mainstream backbones in computer vision. To be specific, we replace the standard convolution in ResNet-18 with the orthogonal convolutions based on BCOP, SOC and ECO. As shown in Table 7, the orthogonal convolution can not achieve the high recognition accuracy as its standard counterpart. But the advantage of orthogonal convolution layers is their provable robustness in LipConvNet, making them still attractive in scenarios when the recognition robustness is important.

CIFAR10				CIFAR100			
Standard	**BCOP**	**SOC**	**ECO**	**Standard**	**BCOP**	**SOC**	**ECO**
95.10%	92.38%	94.24%	92.85%	**77.60%**	71.16%	74.55%	71.87%

Table 7: The standard accuracy using ResNet-18 backbone.

E TRUNCATED TAYLOR EXPANSION

Note that, the exact matrix exponential (Casado & Martínez-Rubio, 2019) $\exp(\mathbf{A})$ relies on singular value decomposition (SVD), which is not friendly for GPU computing platform. Thus, we adopt the truncated Taylor Expansion (Singla & Feizi, 2021b), $\mathbf{S}_T(\mathbf{A}) = \sum_{i=0}^{T} \frac{\mathbf{A}^i}{i!}$, to approximate the exact matrix exponential $\exp(\mathbf{A})$. The truncation error $\mathbf{R} = \exp(\mathbf{A}) - \mathbf{S}_T(\mathbf{A})$ satisfies

$$\|\mathbf{R}\|_2 = \|\exp(\mathbf{A}) - \mathbf{S}_T(\mathbf{A})\|_2 \leq \frac{\|\mathbf{A}\|_2^T}{T!}. \tag{19}$$

Below we first compare the time cost in GPU platform using the exact matrix exponential $\exp(\mathbf{A})$ and that based on the truncated Taylor Expansion $\mathbf{S}_T(\mathbf{A})$. To be specific, we implement $\exp(\mathbf{A})$ simply based on the torch.matrix_exp. We measure the time cost on GPU using the function torch.cuda.Event and we set $T = 10$ in truncated Taylor Expansion $\mathbf{S}_T(\mathbf{A})$. As shown in Table 8, the latency based on the truncated Taylor Expansion is significantly less than that based on the exact matrix exponential.

Exact	Truncated
12.8ms	2.5ms

Table 8: The latency of the exact matrix exponential and the truncated Taylor Expansion in a layer.

Then we show the scale of the average factual truncated error $\mathbf{R}$ with respect to T. It is based on the trained LipConvnet-5 network built upon the proposed ECO convolution. By default, we set $T = 5$ in training and $T = 10$ in testing. As shown in Table 9, the scale of the truncation error is relatively small when T is 5 or 10. Meanwhile, we also show the influence of the truncation error on the orthogonality of the convolution. Following Trockman & Kolter (2021), we measure the orthogonality of a convolution layer through $\frac{\|\text{vec}(\text{conv}(\boldsymbol{\mathcal{X}}))\|_2}{\|\text{vec}(\boldsymbol{\mathcal{X}})\|_2} - 1$, and a strict orthogonal convolution layer should satisfy

$$\frac{\|\text{vec}(\text{conv}(\boldsymbol{\mathcal{X}}))\|_2}{\|\text{vec}(\boldsymbol{\mathcal{X}})\|_2} - 1 = 0. \tag{20}$$

We estimate the deviation of the proposed ECO convolution from the strict orthogonal convolution through this measurement. As shown in Table 9, when T is 5 or 10, the deviation of our ECO convolution from the strict orthogonal convolution is relative marginal.

T	1	2	3	4	5	10
$\|\mathbf{R}\|_2$	0.48	0.16	0.04	0.008	0.001	0.0001
$\frac{\|\mathrm{vec}(\mathrm{conv}(\boldsymbol{\mathcal{X}}))\|_2}{\|\mathrm{vec}(\boldsymbol{\mathcal{X}})\|_2} - 1$	0.12	0.019	0.0038	0.0004	0.0000	0.0000

Table 9: The scale of the average factual truncated error.