Nearest Neighbor Classification Based on Activation Space of Convolutional Neural Network

Speaker: Xinbo Ju



#### Activation Space





### Methodology

Model	MNIST		CIFAR-10	
	TR	TE	TR	TE
LeNet-5	99.39	98.85	78.32	74.65
LeNet-6	99.31	98.67	80.12	75.33

TABLE I: Network accuracy (%) of MNIST and CIFAR-10 on LeNet. **TR**: training accuracy, **TE**: test accuracy.

Model	Top-1 acc.	Top-5 acc.
ResNet50	81.65	96.07
DesNet121	82.41	96.35
VGG16	75.39	93.04
Inception_V3	90.85	99.17
Xception	90.36	98.94

TABLE II: Network test accuracy (%) of ImageNet. Network models come from the embedded models of Keras. Test data is composed of randomly choosed 100 images by each class of ImageNet.



#### **Nearest Convex Hull Classifier(NCH)**

- 1. For every image class, input training data into network to get activation space of each layer and calculate their convex hulls. Convex hull  $CH(X_i^c)$  is composed of all activation vectors in  $X_i^c = \{x_{i,1}^c, x_{i,1}^c, \dots, x_{i,m}^c\}$ . We will obtain n convex hulls for each class at every layer, where n is the number of classes.
- 2. Input a test data (whose class information are to be defined) into network and get its corresponding activation vectors  $t_i$  in each layer of the neural network.
- 3. For each layer i and all candidate class C, calculate distance between vector  $t_i$  to  $CH(X_i^C)$ .
- 4. Classify  $t_i$  to be of class C' to which convex hull  $CH(X_i^C)$  it is closest to. Then accuracy will be defined in the usual way, only now instead of one accuracy (at the output layer), we can get accuracy for every layer.

$$d(x,S) = \min_{a_i} \left\| x - \sum_{i=1}^{|S|} a_i x_i \right\|_2$$

s.t. 
$$a_i \ge 0, \sum_{i=1}^{|S|} a_i = 1$$

## **Convex Hull Sampling**



Fig. 1: Accuracy comparison between sampling and unsampling. Test the NCH algorithm in each layer of LeNet-5 using CIFAR-10. The blue bars represent results for unsampled convex hull and orange bars represent sampled cases.

#### **Nearest Centroid Classifier(NCC)**

- 1. 1. 2. Same as steps 1. 2. in NCH
- 2. For every layer *i* and every class *C*, get the centroids for every convex hull in that layer and use  $V_i^C$  to represent it. Then calculate the Euclidean distance between vector  $t_i$  and each  $V_i^C$ .
  - Here centroid is defined as the arithmetic mean of the set of extreme points on the considered convex hull. Note that the convex hull is constructed by randomly sample 1000 vectors rather than the whole set of data.
- 3. Classify the vector  $t_i$  to be of the class whose centroid it is closest to. The rest are the same as step 4) in the NCH.





#### **Activation Space Visualization**



Fig. 2: (a) Original MNIST

#### **Activation Space Visualization**





Fig. 3: Accuracy of NCH classifier and NCC classifer. The solid line represents the accuracy of NCH and the dot line represents the accuracy of NCC.



Fig. 4: Accuracy of NCC on the last stage of ResNet50 with 100 classes of ImageNet. Adding layers are labeled by red markers. The x-axis lables represent the layer names of the last three residual units of ResNet50.



Fig. 5: Contrast between NCC with 1-norm and 2-norm on the softmax layer of ResNet50. Here we implement 1,000 classes of ImageNet. The red line represents the accuracy of ResNet50 itself.



#### 0.9917 0.9894 norm\_1 0.9851 norm 2 0.9828 0.9635 0.9532 0.9351 0.9304 0.9134 0.903 0.8829 0.8298 VGG16 DenseNet121 Inception V3 Xception

#### (a) Top-1 Accuracy

#### (b) Top-5 Accuracy

Fig. 6: Accuracy of NCC with 1-norm and 2-norm on VGG16, DenseNet121, Inception V3, Xception. The red line represents the accuracy of networks itself.

#### **Analysis and Hypothesis**



#### Data Cluster Mapping

Convex Hull Sampling and Dropout

# Thank you for watching!