COMS 4732: Advanced Computer Vision Homework 3

Overview

In this assignment, we'll build a simple convolutional neural network in PyTorch and Train it to recognize natural objects using the CIFAR-10 dataset. Training a classifier on the CIFAR-10 dataset can be regarded as the hello world of image recognition. The structure of this assignment is:

- 1. Introduction
- 2. Setting up the Environment
- 3. Preparing the Data
- 4. Building the Network
- 5. Training the Model and Evaluating the Performance
- 6. Understand the Deep Neural Networks

(The full content can be better viewed in jupyter notebook).

Submission Instructions

- Please submit the notebook (ipynb and pdf) including the output of all cells. Please note that you should export your completed notebook as a PDF (CV2_HW3_UNI.pdf) and upload it to GradeScope.
- Then, please submit the executable completed notebook (CV2_HW3_UNI.ipynb) to Cousework.
- For both files, 1) remember to replace UNI with your own uni; 2) the completed notebook should show your code, as well as the log and image.

Introduction

Object Recognition typically aims to train a model to recognize, identify, and locate the objects in the images with a given degree of confidence. Object recognition is also called image recognition in many other kinds of literature, which is strictly related to computer vision, which we define as the art and science of making computers understand images.

Deep learning has contributed quite a lot to the development of object recognition algorithms and has achieved many surprising results on many benchmark datasets, such as ImageNet, MS COCO, LVIS. Also, different architectures are proposed to improve the accuracy and efficiency of the learned models. As a brief introduction, we first go through some basic concepts in object recognition and give the following tasks:

- 1. Classification.
- 2. Detection.
- 3. Segmentation.

In this assignment, we only dive into the image classification task and we start with a small model on a toy dataset. We do encourage you to explore the other tasks. Here are a few interesting references:

- 1. https://towardsdatascience.com/creating-your-own-object-detector-ad69dda69c85
- 2. https://medium.com/analytics-vidhya/iou-intersection-over-union-705a39e7acef
- **3.** https://www.analyticsvidhya.com/blog/2018/11/implementation-faster-r-cnn-python-object-detection/
- 4. https://blog.paperspace.com/mask-r-cnn-in-tensorflow-2-0/
- 5. https://www.analyticsvidhya.com/blog/2021/05/an-introduction-to-few-shot-learning/

Classification

Classification is an important task in Object recognition and aims to identify what is in the image and with what level of confidence. The general pipeline of this task is straightforward. It starts with the definition of the ontology, i.e. the class of objects to detect. Then, the classification task identifies what is in the image (associated level of confidence) and picks up the class with the highest confidence. Usually, each test image used for classification has one dominant object in the image and we directly use the representation of the whole image for classification.

For the example given above, the classification algorithm will only remember that there is a dog, ignoring all other classes. Similar to classification, tagging also predicts confidence level for each class but aims to recognize multiple ones for a given image. For the example given below, it will try to return all the best classes corresponding to the image.

Detection and segmentation

Once identified what is in the image, we want to locate the objects. There are two ways to do so: detection and segmentation.Detection outputs a rectangle, also called bounding box, where the objects are. It is a very robust technology, prone to minor errors and imprecisions.

Segmentation identifies the objects for each pixel in the image, resulting in a very precise map. However, the accuracy of segmentation depends on an extensive and often time-consuming training of the neural network.

Different from Classification, Detection and Segmentation ask the algorithm to return the location of the objects in the image. However, as no prior is given to predict the location, a set of potential locations/regions are enumerated. Then, the algorithm performs classification and localization prediction on each of the enumerated subregions. To note, the enumerated sub-regions differ from each other regarding the center location, aspect ratio, and size, while all of them are pre-defined by humans and all of the enumerated sub-regions can densely cover the full image. The location prediction is in effect predicting the offset w.r.t. each the sub-region.

For object detection/segmentation, the two-stage and the one-stage frameworks have been dominating the related research area. Recently, the end-to-end object detector has been proposed to perform prediction in a unified manner (i.e., no pre-defined sub-region will be densely enumerated).

Setting up the Environment

import os

To learn a deep neural network, we need to first build proper environment and we use Pytorch. For some basic overview and features offered in Colab notebooks, check out: Overview of Colaboratory Features.

For this homework, you may need you Colab for your experiments. Under your columbia account, you can open the colab and then upload this jupyter notebook. You need to use the Colab GPU for this assignment by selecting:

Runtime → Change runtime type → Hardware Accelerator: GPU

You should be capable to directly run the following cells in most cases. However, in case you need, you can use the following code to install pytorch when you open the CoLab.

```
!pip install torch torchvision
!pip install Pillow==4.0.0
Below are some input statements which basically imports numpy, torch,
torchvision, matplotlib - This is a known standard and no need to
memorise this
import cv2
import torch
import torchvision
import torchvision.transforms as transforms
from torchvision.datasets import CIFAR10
from torch.utils.data import DataLoader
import torchvision.models as models
import matplotlib.pyplot as plt
import numpy as np
from copy import deepcopy
from torchvision.utils import make grid
import keras
from keras.models import Sequential
import torch.nn as nn
import torch.nn.functional as F
import torch.optim as optim
from torch.utils.data import random split
import math
```

```
import argparse
import time
Warm-Up for Pytorch
#Pytorch is very similar to numpy. Basically, any operation in numpy
can be easily refered for pytorch operations
# The following is a few examples.
# Operations
y = torch.rand(2, 2)
x = torch.rand(2, 2)
# multiplication
z = x * y
z = torch.mul(x,y) #elementwise #must be broadcastable
#matrix multiplication
tensor1 = torch.randn(3, 4)
tensor2 = torch.randn(4, 3)
torch.matmul(tensor1, tensor2)
# NumPy conversion
x = torch.rand(2,2)
y = x.numpy()
print(type(y))
z1 = torch.from numpy(y) #sharing the memory space with the numpy
ndarray
z2 = torch.tensor(y) #a copy
print(type(z1))
print(type(z2))
# Pytorch attributes and functions for tensors
print(x.shape)
print(x.device)
# autograd
# requires grad equals true lets us compute gradients on the tenor
x = torch.tensor([2,3,5], dtype=float, requires_grad=True)
y = (5 * x**2).sum()
# When we finish our computation we can call .backward() and have all
the gradients computed automatically
# The gradient for this tensor will be accumulated into .grad
attribute
y.backward()
#print(z.grad) # dz/dz
print(x.grad) # dz/dx
```

```
# autograd requires computational resources and can take time.
# disable autograd for model eval by writing your evaluation code in
# As such, with torch.no_grad() is usually used in evaluation part

<class 'numpy.ndarray'>
<class 'torch.Tensor'>
<class 'torch.Tensor'>
torch.Size([2, 2])
cpu
tensor([20., 30., 50.], dtype=torch.float64)
```

For repeatable experiments, we are recommended to set random seeds for anything using random number generation - this means numpy and random as well! It's also worth mentioning that cuDNN uses nondeterministic algorithms which can be disabled by setting torch.backends.cudnn.enabled = False.

```
experiment_name = 'debug' #Provide name to model experiment
model_name = 'basic' # Choose between [basic, alexnet]
batch_size = 5 #You may not need to change this but incase you do

torch.manual_seed(42)
<torch._C.Generator at 0x1f5c82e93b0>
```

Preparing the Data

We provide the data-loading functions and a few helper functions below.

To learn a deep learning algorithm, we need to prepare the data and this is where TorchVision comes into play. Usually, we have a training dataset and a test dataset. Each image in the training dataset is paired with a class label, serving as groundtruth to guide the updating of the deep neural network. In real-world test scenario, no label will be provided. However, we still have the labels in the test set to calculate the accuracy. Then, the accuracy on test data is used to quantitatively evaluate the performance, i.e., the generalization of the learned deep algorithm. After all, it will be unexpected if the model works perfectly on the training data but fails on the testing data.

During network training, we usually perform data augmentation on the training data by manipulating the value of pixels. To determine how we adjust the pixel values, we first determine the effects to be applied to the images. TorchVision offers a lot of handy transformations, such as cropping or normalization. For example, shifting the image, adjusting the light and contrast of an image, translating an RGB image into a grayscale image, image rotation, and so on. Also, torchvision can apply random sections among the effects.

To note, the effects to be added on the training data should also seriously consider the property of the dataset. For example, for the digit recognition in MNIST, can we perform 180-degree rotation on the image of digit 6 without altering the image label during network training?

```
def get transform(model name):
    if model name == 'alexnet':
        transform = transforms.Compose([
            transforms.Resize((227, 227)),
            transforms.ToTensor(),
            transforms.Normalize((0.5, 0.5, 0.5), (0.5, 0.5, 0.5)),
        ])
    else:
        transform = transforms.Compose([
            transforms.ToTensor(),
            transforms.Normalize((0.5, 0.5, 0.5), (0.5, 0.5, 0.5)),
        1)
    return transform
def get_dataset(model_name, train_percent=0.9):
    Returns the train, val and test torch. Datasetin addition to a list
of classes, where the idx of class name corresponds
    to the label used for it in the data
    Reference for transforms in torchvision:
https://pytorch.org/vision/stable/transforms.html
   @model_name: either 'basic' or 'alexnet'
    Otrain percent: percent of training data to keep for training.
Rest will \overline{b}e validation.
    transform = get transform(model name)
    train_data = CIFAR10(root='./data', train=True,
download=first run, transform=transform)
    test data = CIFAR10(root='./data', train=False,
download=first run, transform=transform)
    train size = int(train percent * len(train data))
    val size = len(train data) - train size
    train data, val data = random split(train data, [train size,
val size])
    class names = ('plane', 'car', 'bird', 'cat', 'deer', 'dog',
'frog', 'horse', 'ship', 'truck')
```

```
return train data, val data, test data, class names
def get dataloader(batch size, num workers=1, model name='basic'):
    Returns the train, val and test dataloaders in addition to a list
of classes, where the idx of class name corresponds
    to the label used for it in the data
    Reference for dataloader class:
https://pytorch.org/docs/stable/data.html
    @batch size: batch to be used by dataloader
    @num workers: number of dataloader workers/instances used
    @model name: either 'basic' or 'alexnet'
    train set, val set, test set, class names =
get dataset(model name)
    trainloader = DataLoader(train set, batch size=batch size,
shuffle=True, num workers=num workers, pin memory=True)
    valloader = DataLoader(val set, batch size=batch size,
shuffle=False, num workers=num workers, pin memory=True)
    testloader = DataLoader(test_set, batch_size=batch_size,
shuffle=False, num workers=num workers, pin memory=True)
    return trainloader, valloader, testloader, class names
def makegrid images(model name='basic'):
    For visualization purposes
    @model_name: either 'basic' or 'alexnet'
     , trial_loader, _, _ = get_dataloader(32, model_name=model_name)
    images, labels = iter(trial loader).next()
    grid = make grid(images)
    return grid
def show img(img, mean=(0.5, 0.5, 0.5), std=(0.5, 0.5, 0.5), viz=True,
norm=True):
    For visualization purposes
    B: batch size
    C: channels
```

```
H: height
    W: width
    @img: torch.Tensor for the image of type (B, C, H, W)
    @mean: mean used for normalizing along 3 dimensions C, H, W in
get transform
    @std: std. deviation used for normalizing along 3 dimensions C,
H, WW in get transform
   @viz: whether or not to plt.plot or just return the unnormalized
image
   @norm: whether or not unnormalize. Unnormalizes if true.
    Returns:
    Viewable image in (H, W, C) as a numpy array
    if norm:
        for idx in range(img.shape[0]):
            img[idx] = img[idx] * std[idx] + mean[idx]
    image = np.asarray(img)
    if viz:
        if len(image.shape) == 4:
            image = image.squeeze()
        plt.imshow(np.transpose(image, (1, 2, 0)))
        plt.show()
    return np.transpose(image.squeeze(), (1, 2, 0))
```

Building the Network

The network is essentially the key component of the deep learning design. For image classification, the network is typically a convolution neural network (i.e., CNN, ConvNet). CNN will take the full image as input and then predict the confidence level for each class, which is further used for classification. To learn a deep neural network, there are roughly two different ways, 1) training from scratch and 2) finetuning from a pre-trained model.

Training from scratch

First, we will train a shallow convolutional neural network from scratch for practice. We first define the neural network in **GradBasicNet**, randomly initialize the value of the parameters in the network (the reason why it is called "from scratch"), and train it on the training dataset:

- 1. Fill out <code>get_conv_layers()</code> with a network of <code>2 conv layers</code> each with kernel size of <code>5</code>. After the first convolutional layers, add a <code>max pooling layer</code> with kernel size of <code>2 and stride</code> of <code>2</code>. Remember to add the non linearities immediately after the conv layers. You must choose the in-channels and out-channels for both the layers yourself: remember that the image to be input will be RGB so there is only one number that can be used for the in-channels of the first conv layer. Use the <code>nn.Sequential API</code> to combine all this into one layer, and return from <code>get_conv_layers()</code> method
- 2. Fill out **final_pool_layer()** with a max pooling layer. Typically after all the convolutional layers there is another max pooling layer. Use the same kernel size and stride as before and this time directly return the **nn.MaxPool2d**.
- 3. Fill out the **get_fc_layers()** method with a classifier containing 3 linear layers. Once again you are free to choose the in_channels and out_channels for these yourself. Once again use the **nn.Sequential** API and return the object from the method. Inside, alternate the Linear layers with ReLU activations. You do not need a ReLU after the final layer. Remember that the first Linear layer must take in the output of the final convolution layer so depending on your choice in (1.) there is only 1 value you can have for the in_channels of the first Linear layer. Also remember that the final Linear layer must have out_channels=10 as we are performing 10-way classification. Lastly, **remember to leave comments** on why you need to keep the relu of the first two layers while remove the relu of the last layer.
- 4. Finally, you should fill out the forward pass using these layers. Remember to use **self.conv_model**, **self.final_max_pool** and **self.fc_model** one after the other.

Here are a few useful reference for your implementation, which are useful for your implementation:

convolution layers:
 https://pytorch.org/docs/stable/generated/torch.nn.Conv2d.html

2. mas pooling layers: https://pytorch.org/docs/stable/generated/torch.nn.MaxPool2d.html

 ${\it 3.} \quad {\it Sequential API:} \\ \quad {\it https://pytorch.org/docs/stable/generated/torch.nn. Sequential. html}$

class GradBasicNet(nn.Module):

```
def __init__(self):
    super().__init__()

    self.conv_model = self.get_conv_layers()
    self.final_max_pool = self.final_pool_layer()
    self.fc_model = self.get_fc_layers()

def get_conv_layers(self):

#TODO: Group the convolutional layers using nn.Sequential
```

```
layers = nn.Sequential(nn.Conv2d(3,64,kernel size=5),
                              nn.ReLU(),
                              nn.MaxPool2d(kernel_size=2,stride=2),
                              nn.Conv2d(64,128, kernel size=5),
                              nn.ReLU(),)
       return layers
   def final pool layer(self):
       #TODO Set this to a MaxPool layers
       layer = nn.MaxPool2d(2,2)
       return layer
   def get_fc_layers(self):
       # TODO Group the linear layers using nn. Sequential
       layers = nn.Sequential(nn.Linear(in features = 3200,
out features = 2048),
                              nn.ReLU(),
                              nn.Linear(in features = 2048,
out features = 1024),
                              nn.ReLU(),
                              nn.Linear(in_features= 1024,
out features = 10),)
       # Your comment here
       return layers
   def register_grad_hook(self, grad):
       self.grad = grad
   def forward(self, x):
       #TODO
       x = self.conv model(x)#call the conv layers
       #ignore this: relevance for gradcam section
       h = x.register_hook(self.register_grad_hook)
       x = self.final_max_pool(x)#call the max pool layer
       x = torch.flatten(x,1,-1) # flatten the output of x
         print(x.size())
       x = self.fc model(x)#call the fully connected layers
         print(x)
```

```
return x
    def get gradient activations(self):
        return self.grad
    def get final conv layer(self, x):
        return self.conv model(x)
my model = GradBasicNet()
print(my model)
GradBasicNet(
  (conv model): Sequential(
    (0): Conv2d(3, 64, kernel size=(5, 5), stride=(1, 1))
    (1): ReLU()
    (2): MaxPool2d(kernel size=2, stride=2, padding=0, dilation=1,
ceil mode=False)
    (3): Conv2d(64, 128, kernel size=(5, 5), stride=(1, 1))
    (4): ReLU()
  (final max pool): MaxPool2d(kernel size=2, stride=2, padding=0,
dilation=1, ceil mode=False)
  (fc model): Sequential(
    (0): Linear(in features=3200, out features=2048, bias=True)
    (1): ReLU()
    (2): Linear(in features=2048, out features=1024, bias=True)
    (3): ReLU()
    (4): Linear(in features=1024, out features=10, bias=True)
  )
```

Finetuning on a pre-trained model

Secondly, we build a stronger convolutional neural network by starting from a pre-trained model **AlexNet**:

In this subsection, we might have to take advantage of a pretrained network in a process called transfer learning, where we only train a few final layers of a neural network. Here we will use the AlexNet architecture (Krizhevsky et al.)that revolutionized Deep Learning. The pretrained model (on ImageNet) is available on torchvision library and all we need to is ask PyTorch to allow updates on a few of thee final layers during training. We will put the AlexNet model also into the API we have used for our model allow, except that we will need an additionl **transition layer** function for the added **AvgPool** layer. Visualize the model by running the code cell. You will notice:

- 1. (features) contains most of the conv layers. We need upto (11) to include every conv layer
- 2. (features) (12) is the final max pooling layer
- 3. (avgpool) is the transition average pooling layer

4. (classifier) is the collection of linear layers

Question

After you finish the implementation and run the experiments, pls go back and answer the questions below:

- 1. what is the main difference between finetuning and training from scratch.
- 2. Compare the performance between finetuning from a pre-trained model and training from scratch. Explain why the better one outperforms the other?

```
example model = models.alexnet(pretrained=True)
print(example model)
AlexNet(
  (features): Sequential(
    (0): Conv2d(3, 64, \text{kernel size}=(11, 11), \text{stride}=(4, 4),
padding=(2, 2)
    (1): ReLU(inplace=True)
    (2): MaxPool2d(kernel_size=3, stride=2, padding=0, dilation=1,
ceil mode=False)
    (3): Conv2d(64, 192, kernel size=(5, 5), stride=(1, 1),
padding=(2, 2))
    (4): ReLU(inplace=True)
    (5): MaxPool2d(kernel size=3, stride=2, padding=0, dilation=1,
ceil mode=False)
    (6): Conv2d(192, 384, kernel size=(3, 3), stride=(1, 1),
padding=(1, 1)
    (7): ReLU(inplace=True)
    (8): Conv2d(384, 256, kernel size=(3, 3), stride=(1, 1),
padding=(1, 1)
    (9): ReLU(inplace=True)
    (10): Conv2d(256, 256, \text{kernel size}=(3, 3), \text{stride}=(1, 1),
padding=(1, 1)
    (11): ReLU(inplace=True)
    (12): MaxPool2d(kernel size=3, stride=2, padding=0, dilation=1,
ceil mode=False)
  (avgpool): AdaptiveAvgPool2d(output size=(6, 6))
  (classifier): Sequential(
    (0): Dropout(p=0.5, inplace=False)
    (1): Linear(in features=9216, out features=4096, bias=True)
    (2): ReLU(inplace=True)
    (3): Dropout(p=0.5, inplace=False)
    (4): Linear(in features=4096, out features=4096, bias=True)
    (5): ReLU(inplace=True)
    (6): Linear(in features=4096, out features=1000, bias=True)
  )
)
```

Your task is two fold:

1. Implement the method **activate training layers** which sets the requires_grad of relevant parameters to True, so that training can occur. You can iterate over training parameters with

```
for name, param in self.conv_model.named_parameters():
and
for name, param in self.fc model.named parameters():
```

For the conv layers, every param should have requires_grad set to false except for the last layer (10). For the linear layers, all layers must be trainable aka requires_grad must be set to True.

- 1. Implement the forward pass in the following order: self.conv_model, self.final_max_pool, self.avg_pool, self.fc_model
- 2. Remember to fill in your comments under the question mentioned above.

class GradAlexNet(nn.Module):

```
def init__(self):
       super().__init__()
       self.base alex net = models.alexnet(pretrained=True)
       self.conv model = self.get conv layers()
       self.final max pool = self.final pool layer()
       self.avg_pool = self.transition layer()
       self.fc model = self.get fc layers()
       self.activate_training_layers()
   def activate training layers(self):
       #TODO Fill out the function below
       for name, param in self.conv model.named parameters():
           print(name)
           #this is the number of every convolutional layer. From
what model printed above, what is
           #the last convolutional layer?
           # Your comment here
           '''the last convolution layer is: Conv2d(256, 256,
kernel size=(3, 3), stride=(1, 1), padding=(1, 1))
           So, here we are freezing all the convolution layers except
the last layer by setting the requires grad
```

```
to False. Thus the weights of the kernels in these layer
are not updated'''
            number = int(name.split('.')[0])
            # TODO: for all layers except the last layer set
param.requires grad = False
             print(number)
            if number != 10:
                param.requires grad = False
            else:
                param.requires grad = True
        for name, param in self.fc model.named parameters():
            # for all of these layers set param.requires grad as True
            param.requires grad = True
    def get conv layers(self):
        return self.base alex net.features[:12]
    def final pool layer(self):
        return nn.MaxPool2d(kernel size=3, stride=2, padding=0,
dilation=1, ceil mode=False)
    def transition_layer(self):
        return nn.AdaptiveAvgPool2d(output size=(6, 6))
    def get fc layers(self):
        return nn.Sequential(
            nn.Dropout(p=0.5, inplace=False),
            nn.Linear(in features=9216, out features=4096, bias=True),
            nn.ReLU(inplace=True),
            nn.Dropout(p=0.5, inplace=False),
            nn.Linear(in features=4096, out features=4096, bias=True),
            nn.ReLU(inplace=True),
            nn.Linear(in_features=4096, out_features=1000, bias=True),
            nn.ReLU(inplace=True),
            nn.Linear(in features=1000, out features=10, bias=True),
        )
    def register grad hook(self, grad):
        self.grad = grad
    def forward(self, x):
        #TODO fill out the forward pass
        x = self.conv model(x) #call the conv layers
```

```
h = x.register_hook(self.register_grad_hook)

x = self.final_max_pool(x)  #call the max pool layer
    x = self.avg_pool(x)  #call the avg pool layer
    x = torch.flatten(x,1,-1)  # Flatten the output of Avg pool
layer to match the dimensions for the input of FC layer
    x = self.fc_model(x)  #call fully connected layers

    return x

def get_gradient_activations(self):
    return self.grad

def get_final_conv_layer(self, x):
    return self.conv model(x)
```

Training the Model and Evaluating the Model's Performance

Performing network training is intuitive, i.e., feed the training data into the network and then use the groundtruth label to guide the training of the network parameters. In practice, we need to measure the inconsistency between the network output and groundtruth label and then update the network through gradient back propagation. As such, during a network training, a few components are necessary for the implementation.

- 1. criterion (loss function): measure the inconsistency between the network output and label
- 2. optimizer: calculates gradients and then update the network parameters.

Similar to the human vision system which may need to obtain new knowledge by repeating the process of learning and practicing, purely feeding the training data into the model once is far from enough. Meanwhile, we also need to check whether the model overfits to the training data. As such, we monitor the status of the learned network by checking its performance on the test dataset at each training loop.

To note, one training loop is denoted as one epoch and means all of the training data has been used to train the deep neural network once. Now we will fill out the classifier we use to train these networks. Study the general framework for the code below well.

- 1. In the **init** method fill out the **self.criterion** and **self.optimizer**. Remember this is a classification problem so we will need a cross entropy loss. For the optimizer, I would recommend stochastic gradient descent with a learning rate of 0.001 and momentum of 0.9. The rest of **init** has been filled out for you.
- 2. Next, fill out the **training loop**. Here you are expected to iterate over **self.dataloaders['train']** and optimize on the loss with the groundtruth labels. The **validation** aspect of the training loop has been provided for you and so has the evaluate method. In the training loop, print the average loss every 1000 images you process. Remeber to zero out gradients on the model before you do loss.backward(),

and then only after this backward step, make a step in the right direction using the optimizer.

At this stage ignore all methods, after evaluate. They will be relevant to later sections and you will have to return to them when you have more instructions.

```
class Classifier():
    def __init__(self, name, model, dataloaders, class names,
use cuda=False):
        1.1.1
        @name: Experiment name. Will define stored results etc.
        @model: Either a GradBasicNet() or a GradAlexNet()
        @dataloaders: Dictionary with keys train, val and test and
corresponding dataloaders
        @class names: list of classes, where the idx of class name
corresponds to the label used for it in the data
        Quse cuda: whether or not to use cuda
        self.name = name
        if use cuda and not torch.cuda.is available():
            raise Exception("Asked for CUDA but GPU not found")
        self.use cuda = use cuda
        self.model = model.to('cuda' if use_cuda else 'cpu')
        #TODO
        self.criterion = nn.CrossEntropyLoss()#use cross entropy loss
        self.optim = optim.SGD(model.parameters(), lr=0.01)#use SGD
with suggest hyperparams; you must select all the model params
        self.dataloaders = dataloaders
        self.class names = class names
        self.activations_path = os.path.join('activations', self.name)
        self.kernel path = os.path.join('kernel viz', self.name)
        save path = os.path.join(os.getcwd(), 'models', self.name)
        if not os.path.exists(save path):
            os.makedirs(save path)
        if not os.path.exists(self.activations path):
            os.makedirs(self.activations path)
        if not os.path.exists(self.kernel path):
            os.makedirs(self.kernel path)
        self.save path = save path
```

```
def train(self, epochs, save=True):
        @epochs: number of epochs to train
        @save: whether or not to save the checkpoints
        best val accuracy = - math.inf
        for epoch in range(epochs):
            self.model.train()
            batches in pass = len(self.dataloaders['train'])
            #You may comment these two lines if you do not wish to use
them
              loss total = 0.0 # Record the total loss within a few
steps
            epoch loss = 0.0 # Record the total loss for each epoch
            # TODO Iterate over the training dataloader (see how it is
done for validation below) and make sure
            # to call the optim.zero grad(), loss.backward() and
optim.step()
            for idx, data in enumerate(self.dataloaders['train']):
                inputs, labels = data
                inputs = inputs.to('cuda' if self.use_cuda else 'cpu')
                labels = labels.to('cuda' if self.use cuda else 'cpu')
                #Setting Gradient to zero
                self.optim.zero grad()
                # Forward pass to get the Predictions
                outputs = self.model(inputs)
                #Galculate gradient
                loss = self.criterion(outputs, labels)
                # Back propagate the gradient got learning
                loss.backward()
                self.optim.step()
                # update loss
                epoch loss += loss.item()
            '''Give validation'''
            epoch loss /= batches in pass
```

```
self.model.eval()
            #DO NOT modify this part
            correct = 0.0
            total = 0.0
            for idx, data in enumerate(self.dataloaders['val']):
                inputs, labels = data
                inputs = inputs.to('cuda' if self.use_cuda else 'cpu')
                labels = labels.to('cuda' if self.use_cuda else 'cpu')
                outputs = self.model(inputs)
                , predicted = torch.max(outputs, 1)
                total += labels.shape[0]
                correct += (predicted == labels).sum().item()
            epoch accuracy = 100 * correct / total
            print(f'Train Epoch Loss (Avg): {epoch loss}')
            print(f'Validation Epoch Accuracy:{epoch accuracy}')
            if save:
                # Make sure that your saving pipeline is working
well.
                # Is os library working on your file system?
                # Is your model being saved and reloaded fine?
                # When you do the kernel viz, activation maps,
                # and GradCAM you must be using the model you have
saved before.
                torch.save(self.model.state dict(),
os.path.join(self.save path, f'epoch {epoch}.pt'))
                if epoch accuracy > best val accuracy:
                    torch.save(self.model.state dict(),
os.path.join(self.save_path, 'best.pt'))
                    best_val_accuracy = epoch_accuracy
        print('Done training!')
    def evaluate(self):
        try:
            assert os.path.exists(os.path.join(self.save path,
'best.pt'))
```

```
except:
            print('It appears you are testing the model without
training. Please train first')
            return
self.model.load state dict(torch.load(os.path.join(self.save path,
'best.pt')))
        self.model.eval()
        #total = len(self.dataloaders['test'])
        correct = 0.0
        total = 0.0
        mis class = []
        mis predict = []
        for idx, data in enumerate(self.dataloaders['test']):
                inputs, labels = data
                inputs = inputs.to('cuda' if self.use_cuda else 'cpu')
                labels = labels.to('cuda' if self.use cuda else 'cpu')
                outputs = self.model(inputs)
                _, predicted = torch.max(outputs, 1)
                total += labels.shape[0]
                correct += (predicted == labels).sum().item()
                # Updated to store Misclassified images and their true
labels
                for i in range(5):
                    if (predicted[i] != labels[i]):
                        mis class.append(inputs[i])
                        mis predict.append(labels[i])
        print(f'Accuracy: {100 * correct/total}%')
        return mis_class, mis_predict
    def grad cam on input(self, img):
        try:
            assert os.path.exists(os.path.join(self.save path,
'best.pt'))
        except:
            print('It appears you are testing the model without
training. Please train first')
            return
```

```
self.model.load state dict(torch.load(os.path.join(self.save path,
'best.pt')))
        self.model.eval()
        img = img.to('cuda' if self.use_cuda else 'cpu')
        out = self.model(img)
        _, pred = torch.max(out, 1)
        predicted class = self.class names[int(pred)]
        print(f'Predicted class was {predicted class}')
        out[:, pred].backward()
        gradients = self.model.get_gradient_activations()
        print('Gradients shape: ', f'{gradients.shape}')
        mean gradients = torch.mean(gradients, [0, 2, 3]).cpu()
        activations =
self.model.get final_conv_layer(img).detach().cpu()
        print('Activations shape: ', f'{activations.shape}')
        for idx in range(activations.shape[1]):
            activations[:, idx, :, :] *= mean gradients[idx]
        final heatmap = np.maximum(torch.mean(activations,
dim=1).squeeze(), 0)
        final heatmap /= torch.max(final heatmap)
        return final heatmap
    def trained kernel viz(self):
        all layers = [0, 3]
        all filters = []
        for layer in all layers:
            #TODO: blank out first line
            filters = self.model.conv model[layer].weight
            all filters.append(filters.detach().cpu().clone()
```

```
[:8, :8, :, :])
        for filter idx in range(len(all filters)):
            filter = all filters[filter idx]
            print(filter.shape)
            filter = filter.contiguous().view(-1, 1, filter.shape[2],
filter.shape[3])
            image = show img(make grid(filter))
            image = 255 * image
            cv2.imwrite(os.path.join(self.kernel_path,
f'filter_layer{all_layers[filter_idx]}.jpg'), image)
    def activations on input(self, img):
        img = img.to('cuda' if self.use cuda else 'cpu')
        all layers = [0,3,6,8,10]
        all viz = []
        for each in all layers:
            current model = self.model.conv model[:each+1]
            current out = current model(img)
            all viz.append(current out.detach().cpu().clone()
[:, :64, :, :])
        for viz idx in range(len(all viz)):
            viz = all viz[viz idx]
            viz = viz.view(-1, 1, viz.shape[2], viz.shape[3])
            image = show img(make grid(viz))
            image = 255 * image
            cv2.imwrite(os.path.join(self.activations path,
f'sample_layer{all_layers[viz_idx]}.jpg'), image)
Run the classifier for the code using the basic model by running the following snippets. If all
goes well, you should have a test accuracy of about ~60-70% at the end of it. It should take
<10 mins to run on a GPU.
experiment name = 'basic debug' #Provide name to model experiment
model name = 'basic' #Choose between [basic, alexnet]
batch size = 5 #You may not need to change this but incase you do
first run = True #whether or not first time running it
trainloader, valloader, testloader, class names =
get dataloader(batch size=batch size, model name=model name)
dataloaders = { 'train': trainloader, 'val' : valloader, 'test':
```

```
testloader, 'mapping': class names}
if model name == 'basic':
    model = GradBasicNet()
    print(model)
elif model name == 'alexnet':
    model = GradAlexNet()
else:
    raise NotImplementedError("This option has not been implemented.
Choose between 'basic' and 'alexnet' ")
classifier = Classifier(experiment name, model, dataloaders,
class names, use cuda=True)
Files already downloaded and verified
Files already downloaded and verified
GradBasicNet(
  (conv_model): Sequential(
    (0): Conv2d(3, 64, \text{kernel size}=(5, 5), \text{stride}=(1, 1))
    (1): ReLU()
    (2): MaxPool2d(kernel size=2, stride=2, padding=0, dilation=1,
ceil mode=False)
    (3): Conv2d(64, 128, kernel size=(5, 5), stride=(1, 1))
    (4): ReLU()
  (final max pool): MaxPool2d(kernel size=2, stride=2, padding=0,
dilation=1, ceil mode=False)
  (fc model): Sequential(
    (0): Linear(in features=3200, out features=2048, bias=True)
    (1): ReLU()
    (2): Linear(in features=2048, out features=1024, bias=True)
    (3): ReLU()
    (4): Linear(in features=1024, out features=10, bias=True)
  )
)
start time = time.time()
# When you develop your code, to save your time, you can choose to run
the model
# for 5 cpoches. The accuracy after training for 5 epoches has already
been high
# and close to the model after 20-epoch traiing.
# (In my case, Validation Epoch Accuracy is above 61 after training 5
epoches)
# To note, for your final submission, you should make sure to train
the model
# for 20 epoches and analysis that model in the later sections.
# classifier.train(epochs=5) # For your reference -- Gave a testing
```

```
accuracy of 71.09% after removing the Sotmax activation in the last
laver
classifier.train(epochs=20)
classifier.evaluate()
end time = time.time()
seconds = end time-start time
a=str(seconds//3600)
b=str((seconds%3600)//60)
c=str((seconds%3600)%60)
print("Runtime is {} mins {} seconds".format(b, c) )
Train Epoch Loss (Avg): 1.5574012606061167
Validation Epoch Accuracy:55.92
Train Epoch Loss (Avg): 1.0933699692802297
Validation Epoch Accuracy:65.08
Train Epoch Loss (Avg): 0.8453393266325195
Validation Epoch Accuracy:68.2
Train Epoch Loss (Avg): 0.6532648838936972
Validation Epoch Accuracy: 72.68
Train Epoch Loss (Avg): 0.4852819889262852
Validation Epoch Accuracy: 72.6
Train Epoch Loss (Avg): 0.333389713874343
Validation Epoch Accuracy:72.52
Train Epoch Loss (Avg): 0.20685714090993468
Validation Epoch Accuracy:72.72
Train Epoch Loss (Avg): 0.14422926363718164
Validation Epoch Accuracy:73.48
Train Epoch Loss (Avg): 0.10974027555960737
Validation Epoch Accuracy:73.9
Train Epoch Loss (Avg): 0.08006465448408935
Validation Epoch Accuracy:73.82
Train Epoch Loss (Avg): 0.07458920796658128
Validation Epoch Accuracy:73.9
Train Epoch Loss (Avg): 0.050280273188558024
Validation Epoch Accuracy:74.08
Train Epoch Loss (Avg): 0.041066225623856784
Validation Epoch Accuracy:74.1
Train Epoch Loss (Avg): 0.046392964278332935
Validation Epoch Accuracy:73.28
Train Epoch Loss (Avg): 0.04136607586709112
Validation Epoch Accuracy:72.9
Train Epoch Loss (Avg): 0.032189272117269095
Validation Epoch Accuracy:73.14
Train Epoch Loss (Avg): 0.02666429711111452
Validation Epoch Accuracy: 73.58
Train Epoch Loss (Avg): 0.022269068431727386
Validation Epoch Accuracy: 73.16
Train Epoch Loss (Avg): 0.01797059628466838
Validation Epoch Accuracy: 74.92
Train Epoch Loss (Avg): 0.01338294522274264
```

```
Validation Epoch Accuracy:73.06
Done training!
Accuracy: 74.51%
Runtime is 11.0 mins 26.810404062271118 seconds
Now run the classifier for the code using the alexnet model specified above. You should
notice a notable performance increase. On a GPU, this trained for about 30 mins.
experiment name = 'alexnet debug' #Provide name to model experiment
model_name = 'alexnet' #Choose between [basic, alexnet]
batch size = 5 #You may not need to change this but incase you do
first run = True #whether or not first time running it
trainloader, valloader, testloader, class names =
get dataloader(batch size=batch size, model name=model name)
dataloaders = {'train': trainloader, 'val' : valloader, 'test':
testloader, 'mapping': class names}
#model = models.alexnet(pretrained=True)
if model name == 'basic':
    model = GradBasicNet()
elif model name == 'alexnet':
    model = GradAlexNet()
else:
    raise NotImplementedError("This option has not been implemented.
Choose between 'basic' and 'alexnet' ")
classifier = Classifier(experiment name, model, dataloaders,
class names, use cuda=True)
Files already downloaded and verified
Files already downloaded and verified
0.weight
0.bias
3.weight
3.bias
6.weight
6.bias
8.weight
8.bias
10.weight
```

When you develop your code, to save your time, you can choose to run

10.bias

the model

start time = time.time()

```
# for 3 cpoches. The accuracy after training for 3 epoches has already
been high
# and close to the model after 20-epoch traiing.
# To note, for your final submission, it is recommended to run the
model for 20 epochs.
# However, if it takes time, you should at least run the model for 5
epochs.
# classifier.train(epochs=3) # For your reference -- Gave a testing
accuracy of 84.61%
classifier.train(epochs=20)
classifier.evaluate()
end time = time.time()
seconds = end time-start time
a=str(seconds//3600)
b=str((seconds%3600)//60)
c=str((seconds%3600)%60)
print("Runtime is {} mins {} seconds".format(b, c) )
Train Epoch Loss (Avg): 0.04170100553231375
Validation Epoch Accuracy:88.12
Train Epoch Loss (Avg): 0.04461946414260303
Validation Epoch Accuracy:88.0
Train Epoch Loss (Avg): 0.034979839179417375
Validation Epoch Accuracy:87.72
Train Epoch Loss (Avg): 0.03876917195089144
Validation Epoch Accuracy:87.7
Train Epoch Loss (Avg): 0.03701492064506696
Validation Epoch Accuracy:88.12
Train Epoch Loss (Avg): 0.03410998021910295
Validation Epoch Accuracy:88.26
Train Epoch Loss (Avg): 0.030846820597112305
Validation Epoch Accuracy:88.38
Train Epoch Loss (Avg): 0.029447872827568826
Validation Epoch Accuracy:88.6
Train Epoch Loss (Avg): 0.0266833879962032
Validation Epoch Accuracy:88.54
Train Epoch Loss (Avg): 0.02679124284995841
Validation Epoch Accuracy:88.52
Train Epoch Loss (Avg): 0.02774017481920089
Validation Epoch Accuracy:87.88
Train Epoch Loss (Avg): 0.022899085279888
Validation Epoch Accuracy:88.42
Train Epoch Loss (Avg): 0.023341571029144775
Validation Epoch Accuracy:88.22
Train Epoch Loss (Avg): 0.023348210201094143
Validation Epoch Accuracy:88.34
Train Epoch Loss (Avg): 0.019807290920023746
Validation Epoch Accuracy:87.8
```

```
Train Epoch Loss (Avg): 0.021406719919317543
Validation Epoch Accuracy:88.06
Train Epoch Loss (Avg): 0.02175237720757707
Validation Epoch Accuracy:88.08
Train Epoch Loss (Avg): 0.019338472155329543
Validation Epoch Accuracy:88.26
Train Epoch Loss (Avg): 0.018399522826669686
Validation Epoch Accuracy:88.78
Train Epoch Loss (Avg): 0.019653072820309855
Validation Epoch Accuracy:88.86
Done training!
Accuracy: 88.09%
Runtime is 39.0 mins 32.302571296691895 seconds
```

Before you move forward to the next step: Try and see what classes your model does well on (you can modify the testing code for this). This will help you pick the best visualization to show later.

Understand the Deep Neural Networks

The deep learning is quite powerful and can achieve great performance after training for a few epochs. However, we still don't know why it works. Thus, we first study activation map to analysis the region that triggers the final classification. Then, we visualze a few kernels to infer what is learned in the neural network. (The activition map and kernel visualization are two popurlar directions. However, much more effort is still needed to comprehensively understand deep neural networks and reach the ultimate goal.)

Activation Map

For interpreting our alexnet model, we will be using a simple version of Grad-CAM (Gradient based Class activation mapping) by Selvaraju et al.

(https://arxiv.org/abs/1610.02391). This will help us see what region of the input image the output is 'focusing on' while making its key choice. I recommend reading the paper for those interested: however, the following instructions should also suffice. If you go step-by-step then all information is given in the intructions. You will receive one img to the method.

- 1. First, move the img to cuda if you are using GPU.
- 2. The code to load the model trained from before has been provided to you. Use self.model to output the predictions to the variable out. Your output should have dimension (1, 10).
- 3. The predicted class is the index of the highest value of of these 10 values. Use **torch.max** along dim 1 to get the argument of the max value. This method will return two values, the latter of them is the required argument. The next two lines have been provided to you: they indicate the predicted loss
- 4. Call the **backward** method on out[:, pred]. Previously during the forward passes, we have applied a gradient hook on the last convolutional layer. This will mean that during the applied backward pass, we will record the value of the gradient for the **maximum predicted class** with respect to the **output** of the last convolutional

- layer. This will be the same size as the **output** of the last convolutional layer. Do you see why?
- After the **backward** call, get the value of the gradient above using the get_gradient_activations function on self.model and store it in gradients. Now use the torch.mean method to get the mean value of gradients across all dimensionss except the channels dimension (number of filters) and store this in **mean_gradients**. Your output should be of shape (1, 64, 1, 1). If your tensors have been on GPU, you should move them to CPU using .detach().cpu()
- 6. Use the self.model.get_final_conv_layer(img) to store the activations at the final layer to activations. This should be of shape (1, 64, H, W).
- Now for each of the 64 filters, **scale** the activations at that filter, with the corresponding **mean_gradients** value for that filter. Your output should have size (1, 64, H, W) Iterate over the 64 filters in the following way: for idx in range(activations.shape[1]):
- 8. As a final step, we will take mean across the 64 filters and do a ReLU to get rid of negative activations before normalzing one last time to get the heatmap. This has been done for you.

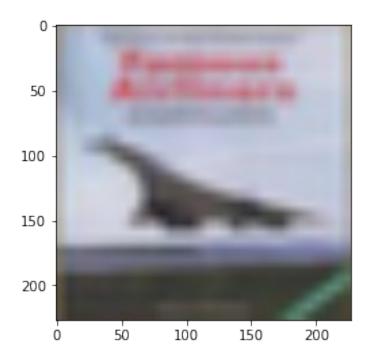
```
'''Sample an image from the test set'''
#You may change the sampling code to sample an image as you desire.
#Make sure to NOT move the sampling code to a different cell.
img batch, labels batch = next(iter(testloader))
img = img batch[3]
img = img.unsqueeze(0)
classifier = Classifier(experiment name, model, dataloaders,
class names, use cuda=True)
heatmap = classifier.grad cam on input(img)
def visualize(img, heatmap):
    heatmap = heatmap.cpu().numpy()
    img = show img(img)
    img = np.uint8(255 * img)
    img = cv2.cvtColor(img, cv2.COLOR BGR2RGB)
    print(img.shape)
    print(heatmap.shape)
    heatmap = cv2.resize(heatmap, (img.shape[1], img.shape[0]))
    heatmap = np.uint8(255 * heatmap)
    heatmap = cv2.applyColorMap(heatmap, cv2.COLORMAP JET)
    heatmap = cv2.cvtColor(heatmap, cv2.COLOR BGR2RGB)
    combine = 0.5 * heatmap + img
```

```
#if not os.path.exists(write_path):
# os.makedirs(write_path)

plt.imshow(combine/255)
plt.show()
```

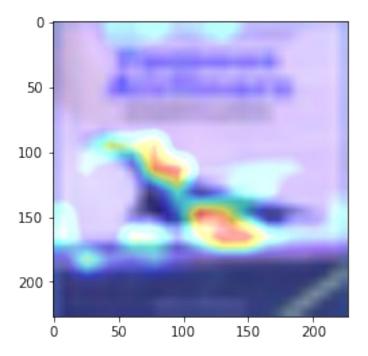
visualize(img, heatmap)

Predicted class was plane Gradients shape: torch.Size([1, 256, 13, 13]) Activations shape: torch.Size([1, 256, 13, 13])



(227, 227, 3) (13, 13)

Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).



Your code here to show a failure case.

What do you observe? Show an example of an image where the method is looking at the object in question and another where it appear to be completely unrelated. In the latter case, it might have learnt a spurious correlation- aka a bias in the data which always appears to be correlated with a given label. For the ship class, this **might** be the surrounding water or for a **horse** it might be the surrounding grass. In such cases, do you think the model would predict correctly for a ship on sand or a horse in the air? Answer in a text snippet below. **Causally trained neural networks**

 $(https://www.cmu.edu/dietrich/causality/neurips 20 ws/) \ are \ an \ exciting \ direction \ to \ solve \ this \ problem$

```
# You can refer the steps and functions implemented in the previous
cell and reuse them.

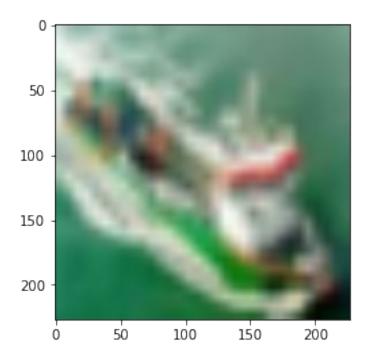
torch.cuda.empty_cache()

classifier = Classifier(experiment_name, model, dataloaders,
class_names, use_cuda=True)

# Get the misclassified Images
mis_img, mis_predict = classifier.evaluate()
Actual_class = class_names[int(mis_predict[0])]
print(f'Actual class was {Actual_class}')

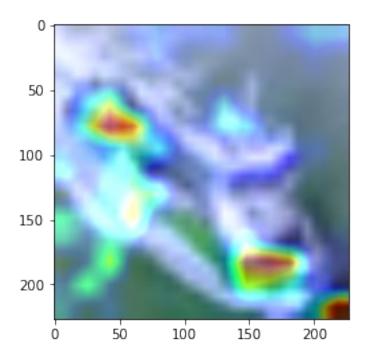
#Using One image as an example
mis_img = mis_img[0]
mis_img = mis_img.unsqueeze(0)
heatmap = classifier.grad_cam_on_input(mis_img)
```

```
def visualize(img, heatmap):
    heatmap = heatmap.cpu().numpy()
    img = img.cpu().numpy()
    img = show img(img)
    img = np.uint8(255 * img)
    imq = cv2.cvtColor(img, cv2.COLOR_BGR2RGB)
    print(img.shape)
    print(heatmap.shape)
    heatmap = cv2.resize(heatmap, (img.shape[1], img.shape[0]))
    heatmap = np.uint8(255 * heatmap)
    heatmap = cv2.applyColorMap(heatmap, cv2.COLORMAP JET)
    heatmap = cv2.cvtColor(heatmap, cv2.COLOR BGR2RGB)
    combine = 0.5 * heatmap + img
    #if not os.path.exists(write_path):
    # os.makedirs(write path)
    plt.imshow(combine/255)
    plt.show()
visualize(mis img, heatmap)
Accuracy: 87.77%
Actual class was ship
Predicted class was frog
Gradients shape: torch.Size([1, 256, 13, 13])
Activations shape: torch.Size([1, 256, 13, 13])
```



Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).

(227, 227, 3) (13, 13)



Answer: The Network classied a ship as a frog with max values in the heat map focus in the background where it is surrounded by water. Thus suggesting that ship is misclassified as frog due to the background which suggests spurious correlation. From the heatmap it is

also visible that most of the activations are in the area where usually the head and tail of the frog is which is a unique identifier. The ConvNet fails to have activations in the recognize which would reveal the shape of the ship.

Kernel and Activation Visualizations

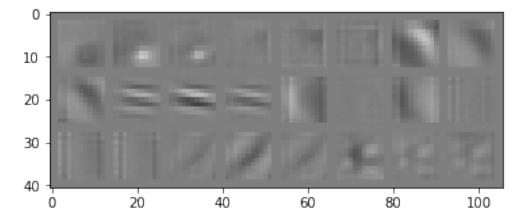
We will visualize some learned convolutional kernels for two layers in the conv-net. Study the code provided for **trained_kernel_viz** carefully. You only have to fill out the line for **filter**. All you are expected to do is to access the relevantt layer from **self.conv_model** and set **filter** equal to its weight parameter.

Call this function on the alexnet classifier. What do you observe?

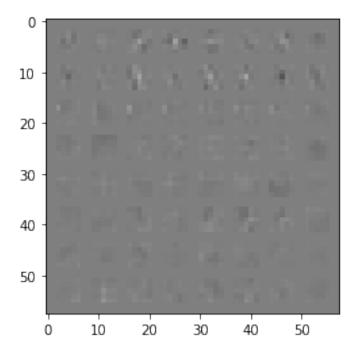
Answer: Since we are visualizing [0, 3] among all layers. The visualized kernels are only for 1st and 4th layers whicjh are convolution layers. The image shown for the first for the 1st layer there are 3 input channels and kernel size is 11×11 , and since we are storing 1st 8 kernels the shape is [8, 3, 11, 11]. And in with similar explaination the filters for 2nd convolution layers shown has sie [8, 8, 5, 5]. We can observe fromt the images of kernel the these kernels would be able to identify edges which is in cohesion to the fact that the first few convolution layers learn to detect low level features such as edges

classifier.trained kernel viz()

torch.Size([8, 3, 11, 11])



torch.Size([8, 8, 5, 5])



Now with the kernel viz filled out, write the method for activation visualizations activations on input. The structure for the code is very similar to the kernel viz, except that we are actually viewing the output of the model at each stage and not for the kernel at that stage. Once filled, please call this method on a few sample images. What do you observe? Answer generally in a text snippet below.

Answer: we observe that for initial layers many zones are activated as it will be detecting low features in the the images, whereas as we move ahead in the model the kernels start learning more high level features such as nose, mouth wings, eyes, etc. thus a smaller portion of the image would be activated.

```
"''Sample an image from the test set'''

#You may change the sampling code to sample an image as you desire.

#Make sure to NOT move the sampling code to a different cell.

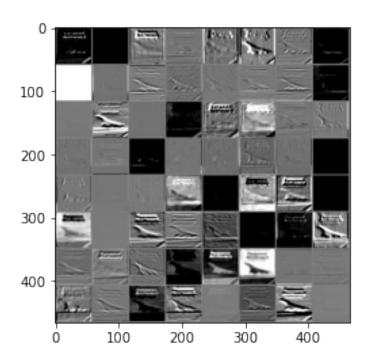
img_batch, labels_batch = next(iter(testloader))

img = img_batch[3]

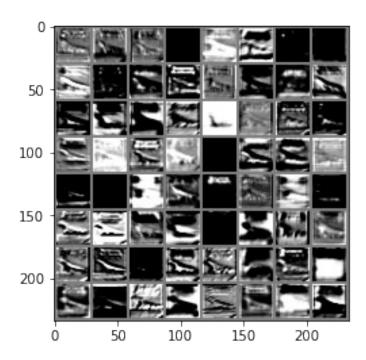
img = img.unsqueeze(0)

classifier = Classifier(experiment_name, model, dataloaders,
class_names, use_cuda=True)
classifier.activations_on_input(img)

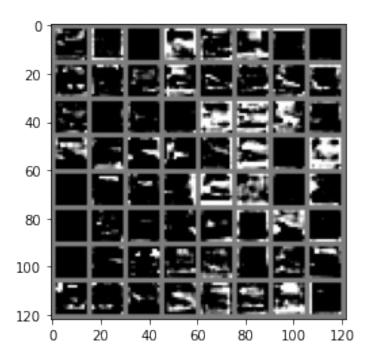
Clipping input data to the valid range for imshow with RGB data
([0..1] for floats or [0..255] for integers).
```



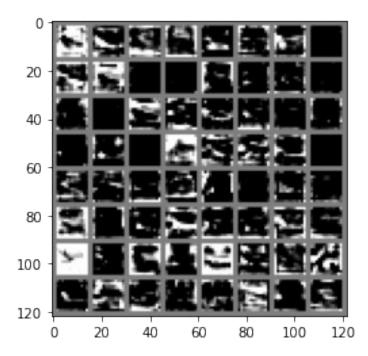
Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).



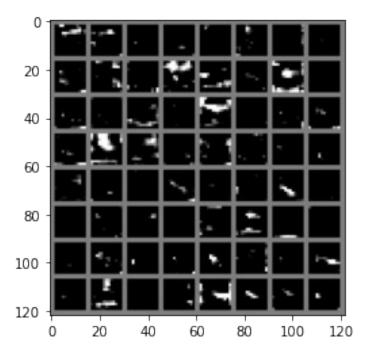
Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).



Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).



Clipping input data to the valid range for imshow with RGB data ([0..1] for floats or [0..255] for integers).



What do you observe about early layers v. later layers? Answer in a text snippet below.

Answer: We observe that early layers learn low level features in images and majority portion of the image is activated whereas on the contrary in the later layers high level features are learned and smaller areas of the images are activated