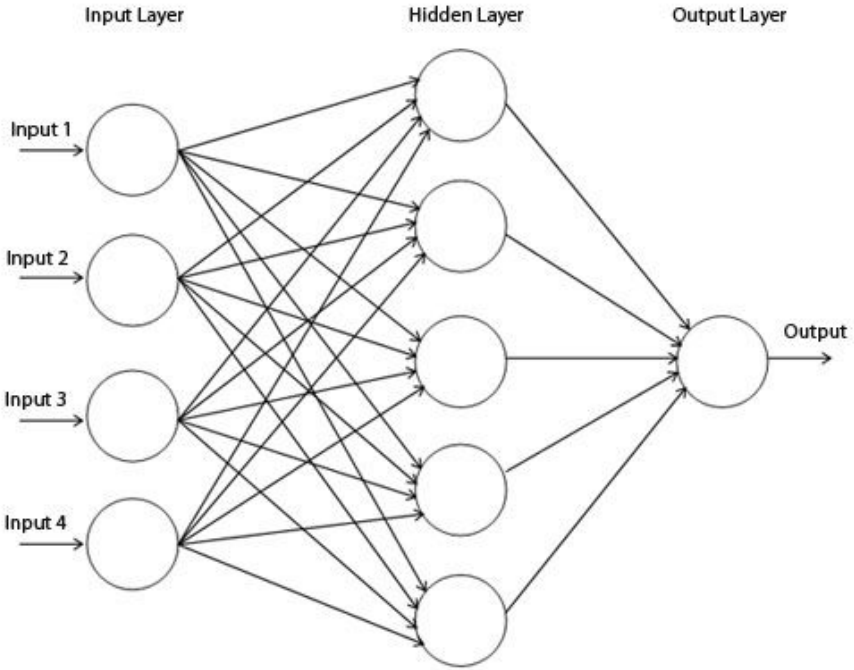
CS21si: AI for Social Good

Lecture 4: Convolutional Neural Networks

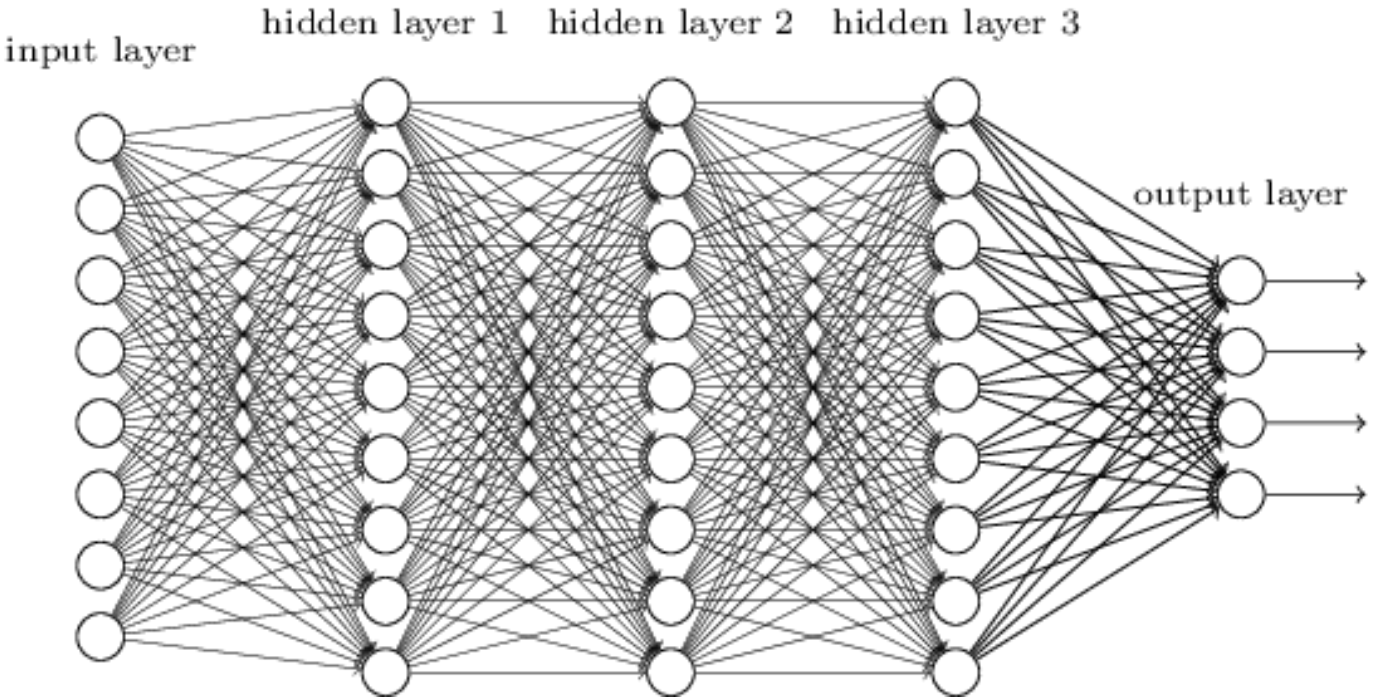
Plan for Today

- Review of deep neural networks
- Convolutional neural networks
- Implementing CNNs
- Adversarial attacks

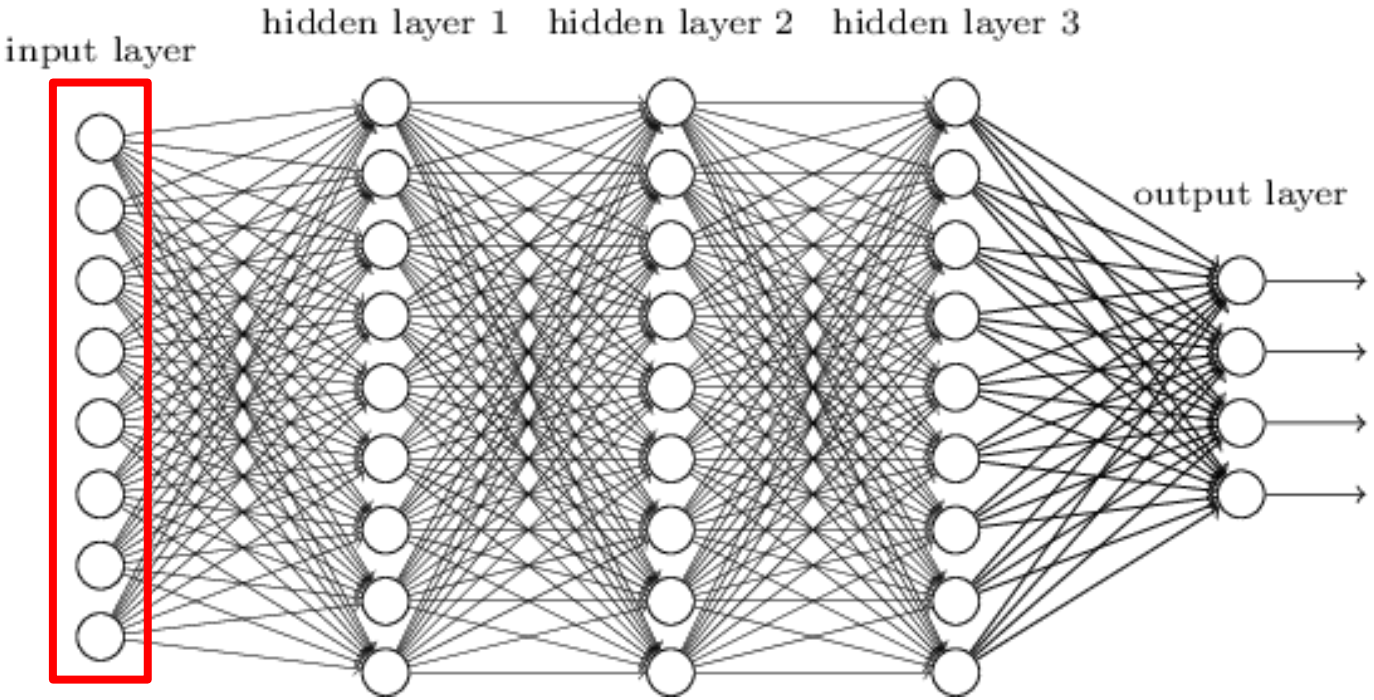
Deep Neural Networks



Deep Neural Networks



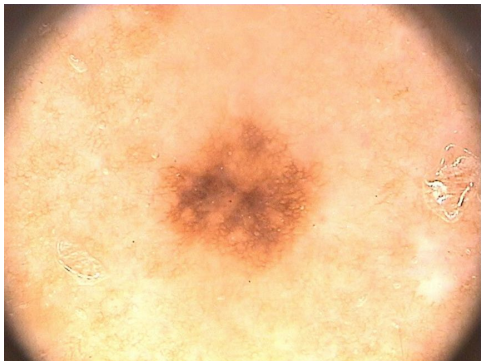
Deep Neural Networks



What sort of input can I give an neural net?

How do I handle image data?

ADDI - Automated Diagnosis for Dermoscopic Images



ADDI - Automated Diagnosis for Dermoscopic Images

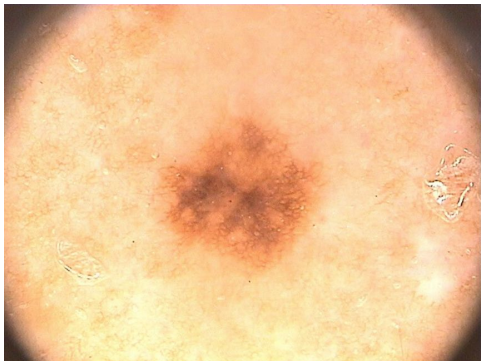
Common Nevus

Atypical Nevus

Melanoma

ADDI - Automated Diagnosis for Dermoscopic Images

Normal



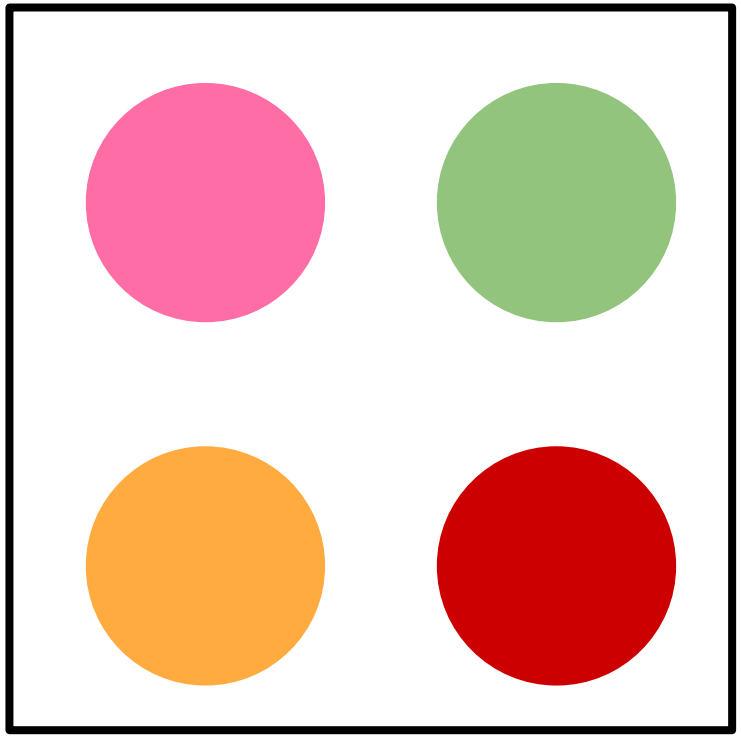
Abnormal

Jupyter Exercises 1: Visualize the Data

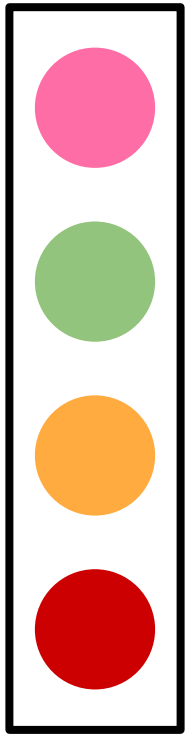
How do I handle image data?

One Idea...

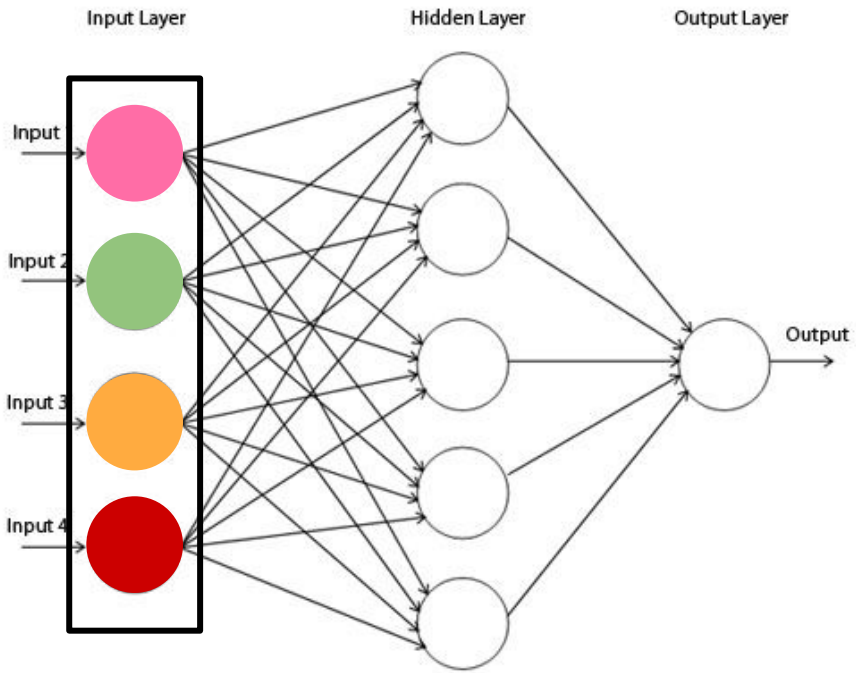
One Idea...



One Idea...

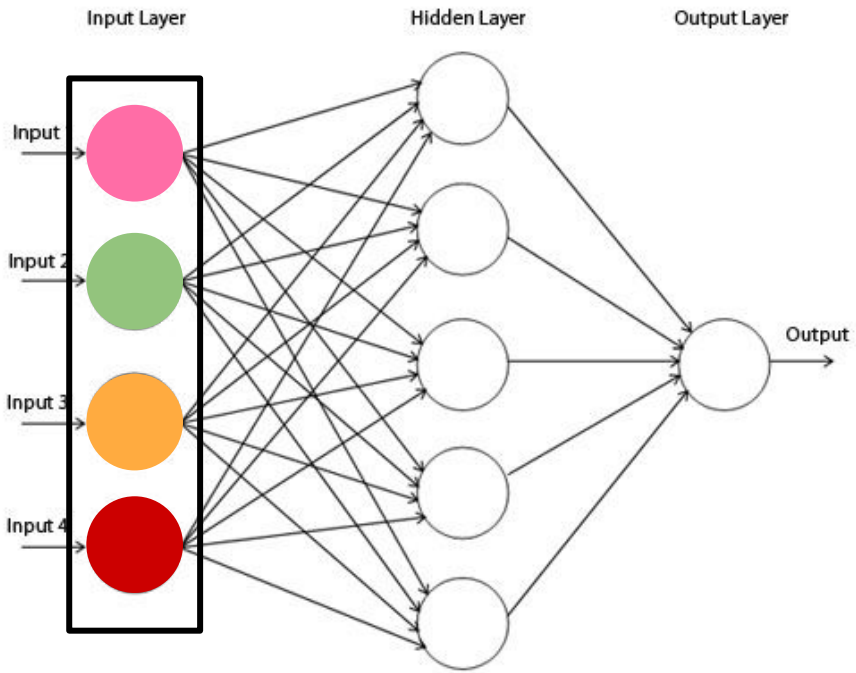


One Idea...


Input Layer
Hidden Layer
Output Layer
Input
Input 2
Input 3
Input 4
Output

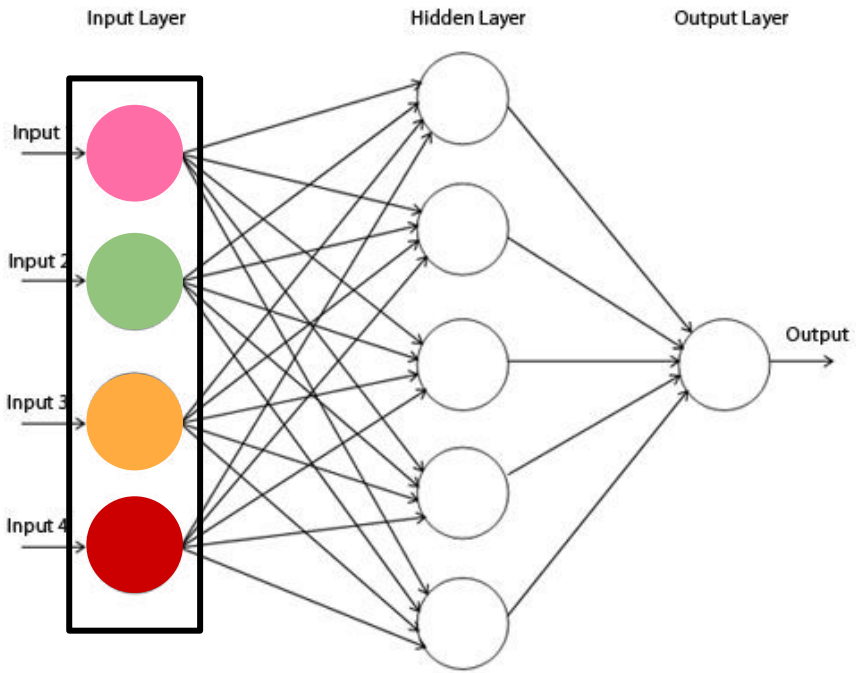
Questions?

Issue with Our Idea



Issue with Our Idea

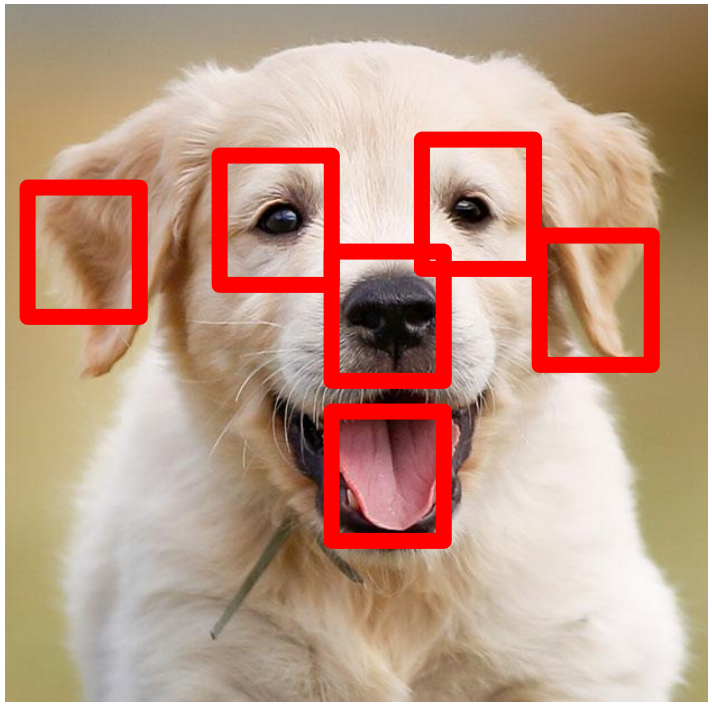
Assumes independence of features (pixels)!



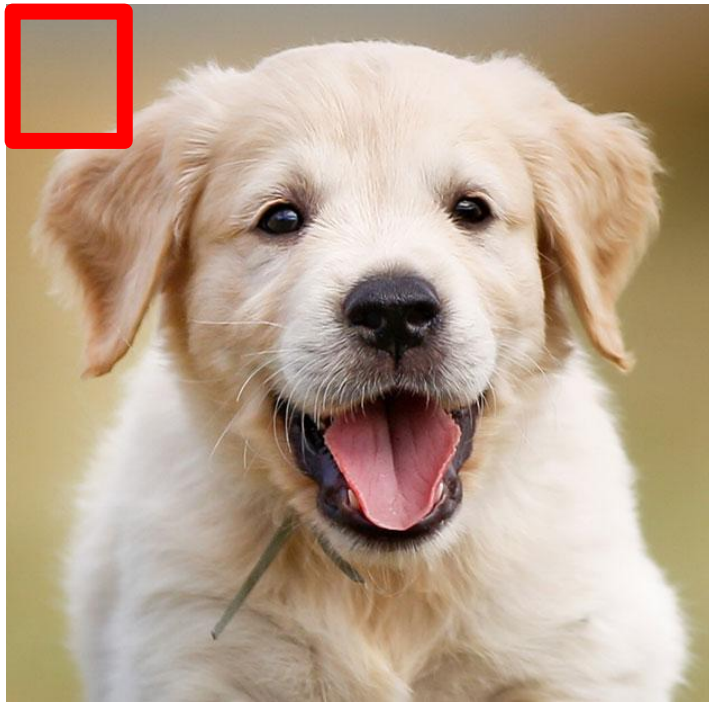
Key Insight: we want to maintain spatial dependence

Windowing

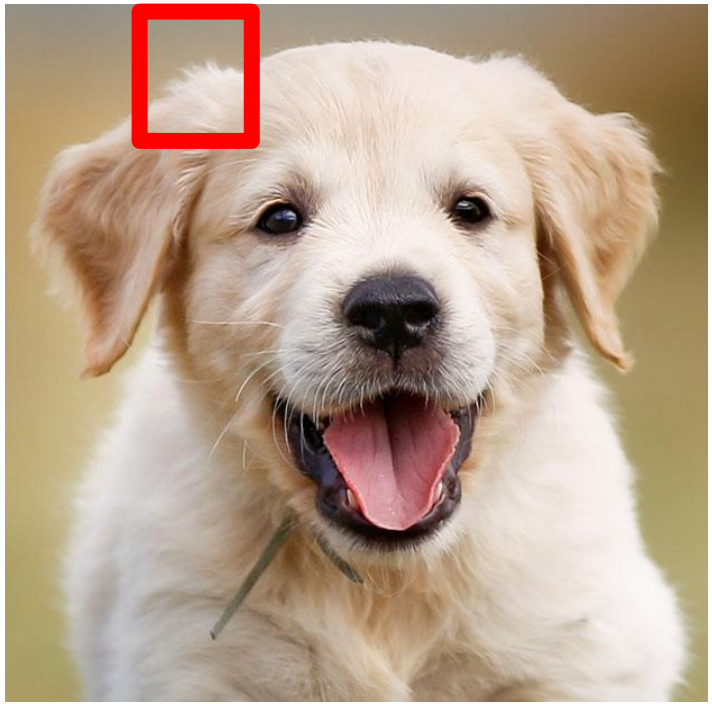
Windowing



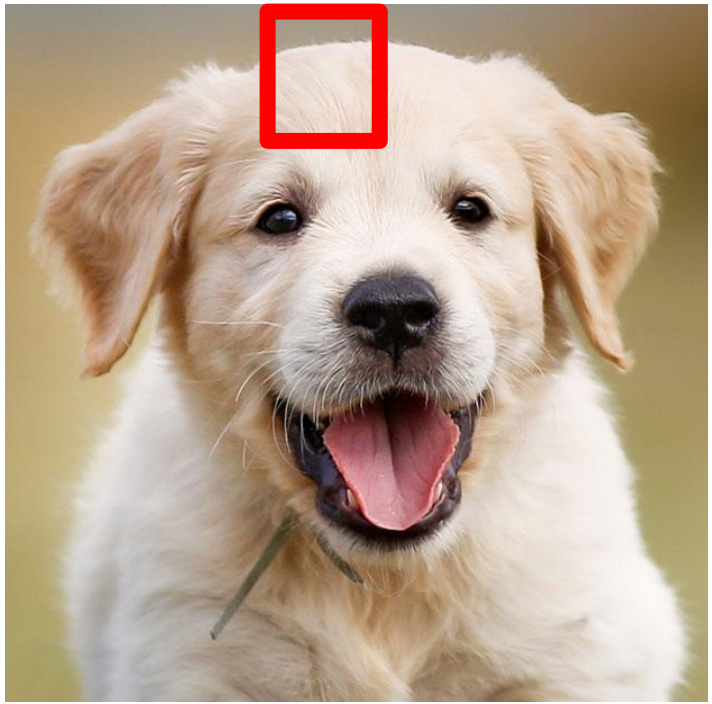
Windowing



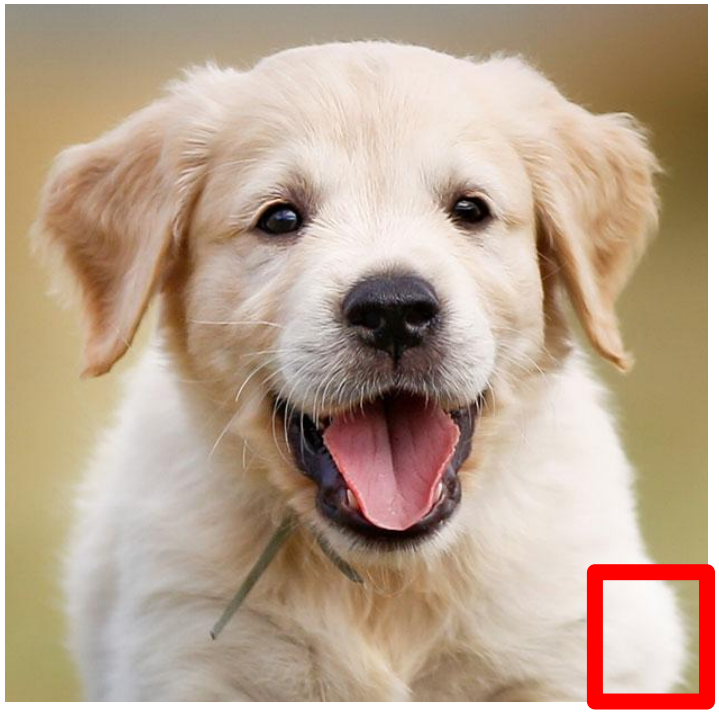
Windowing



Windowing

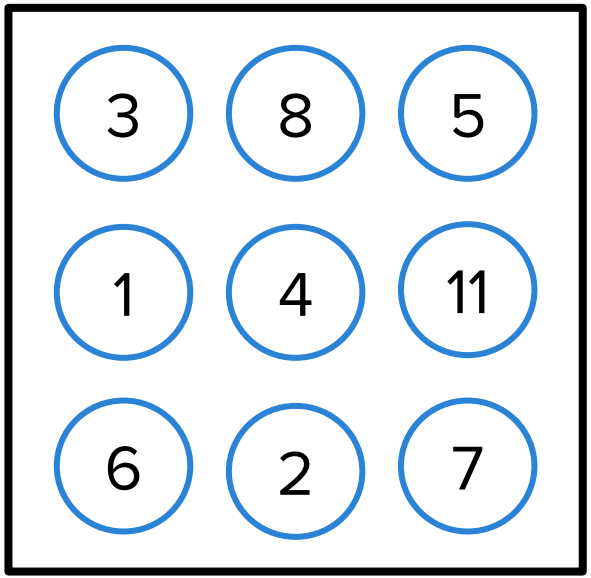


Windowing

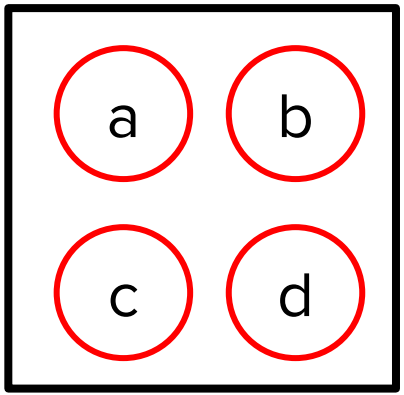


Questions?

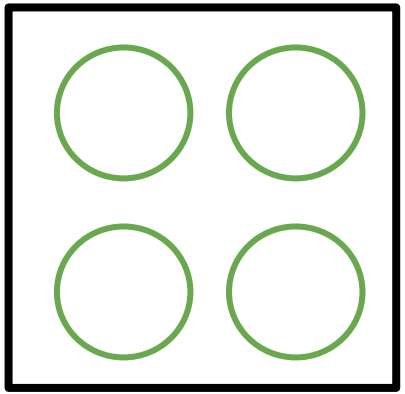
Convolutional Layer



Input

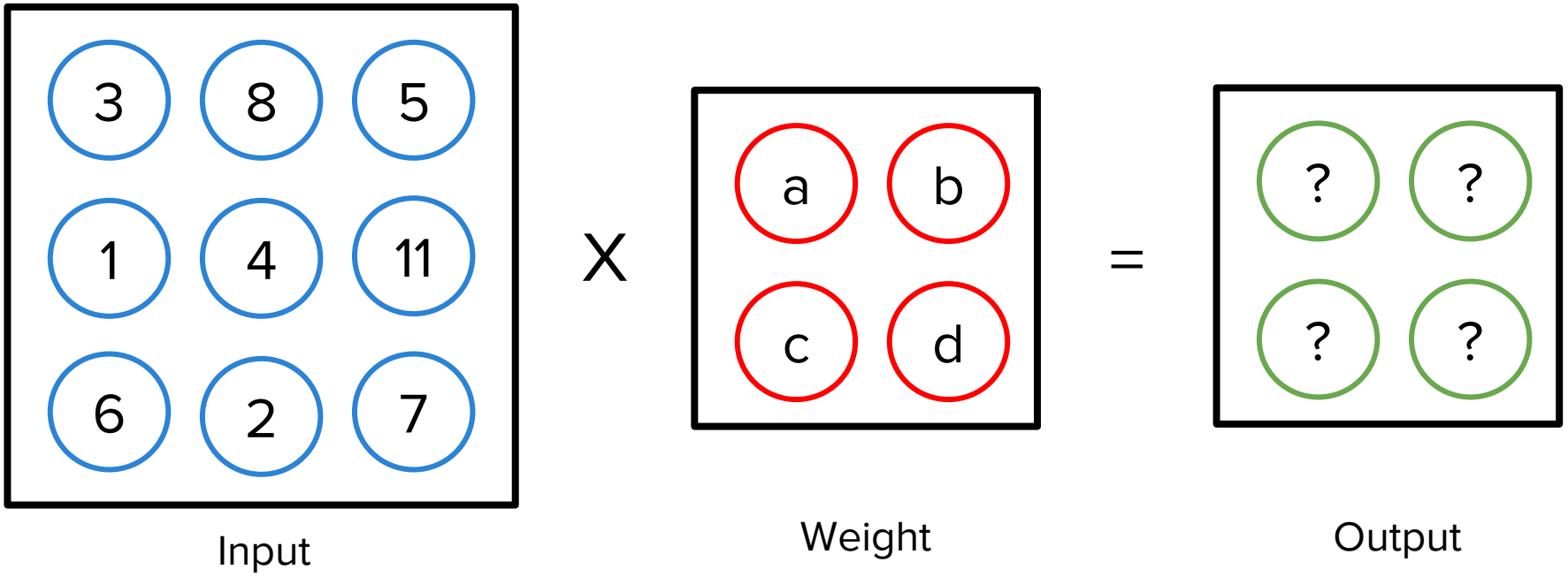


Weight

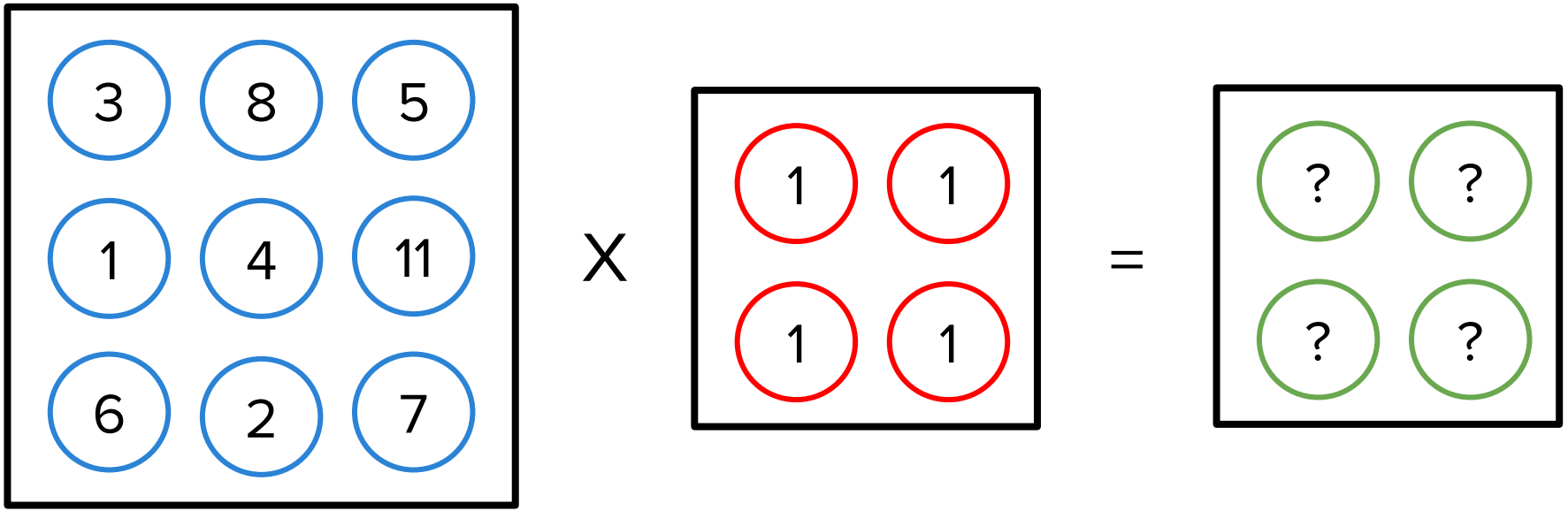


Output

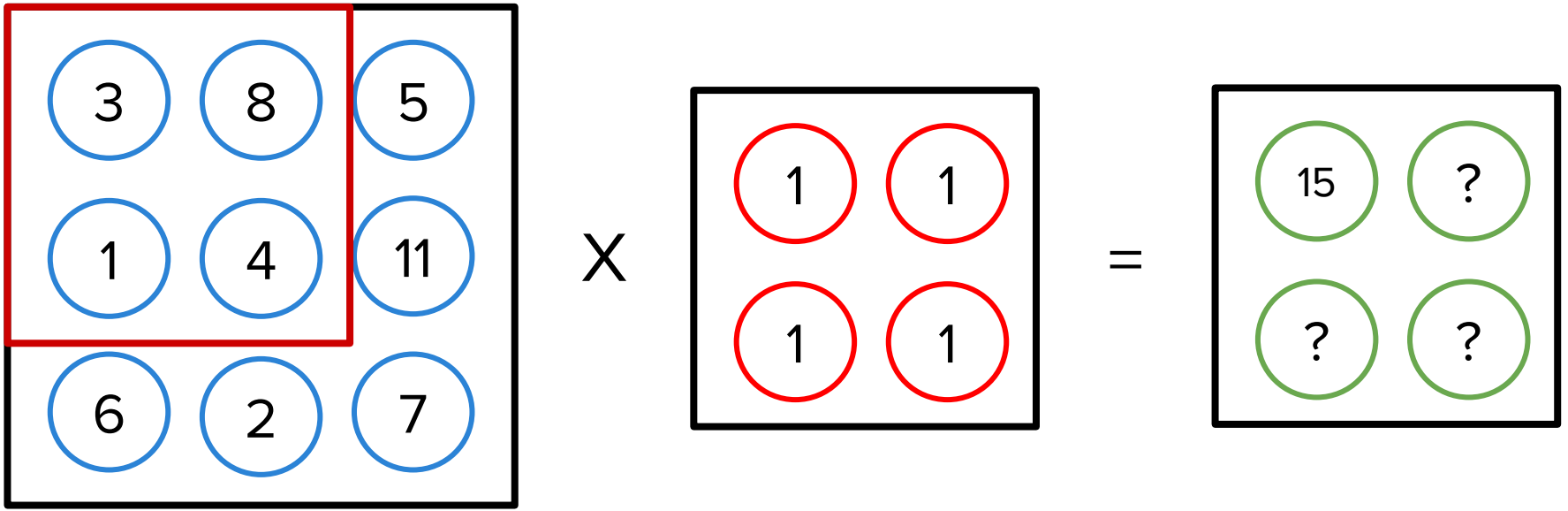
Convolutional Layer



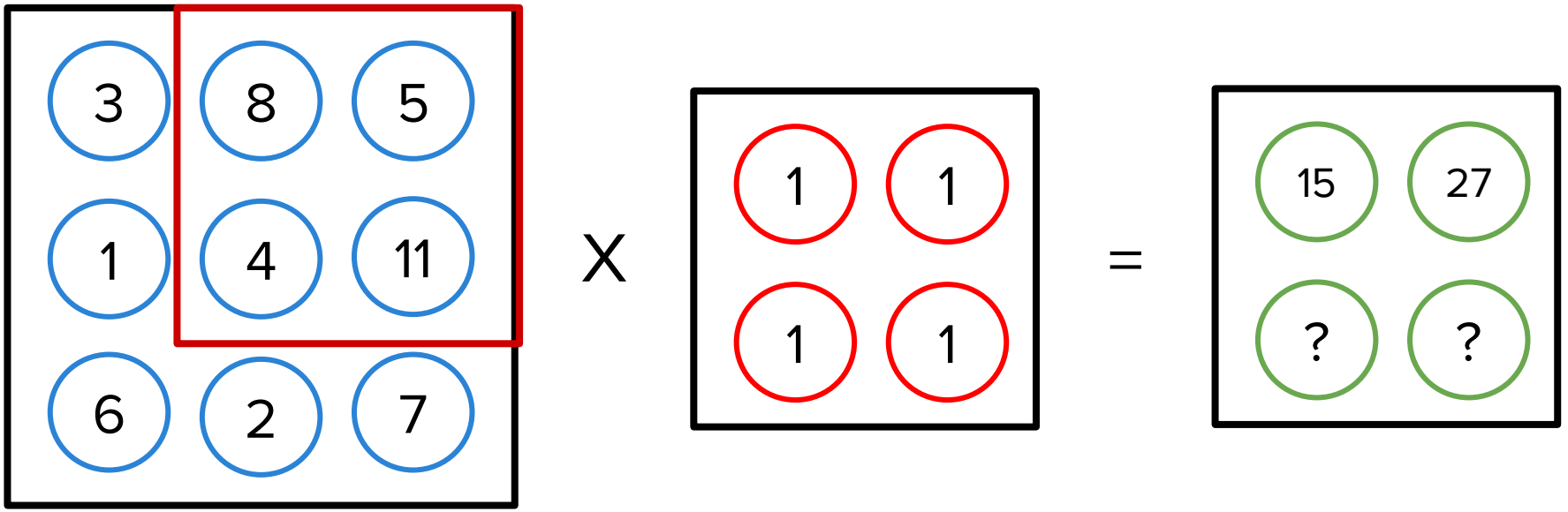
Convolutional Layer



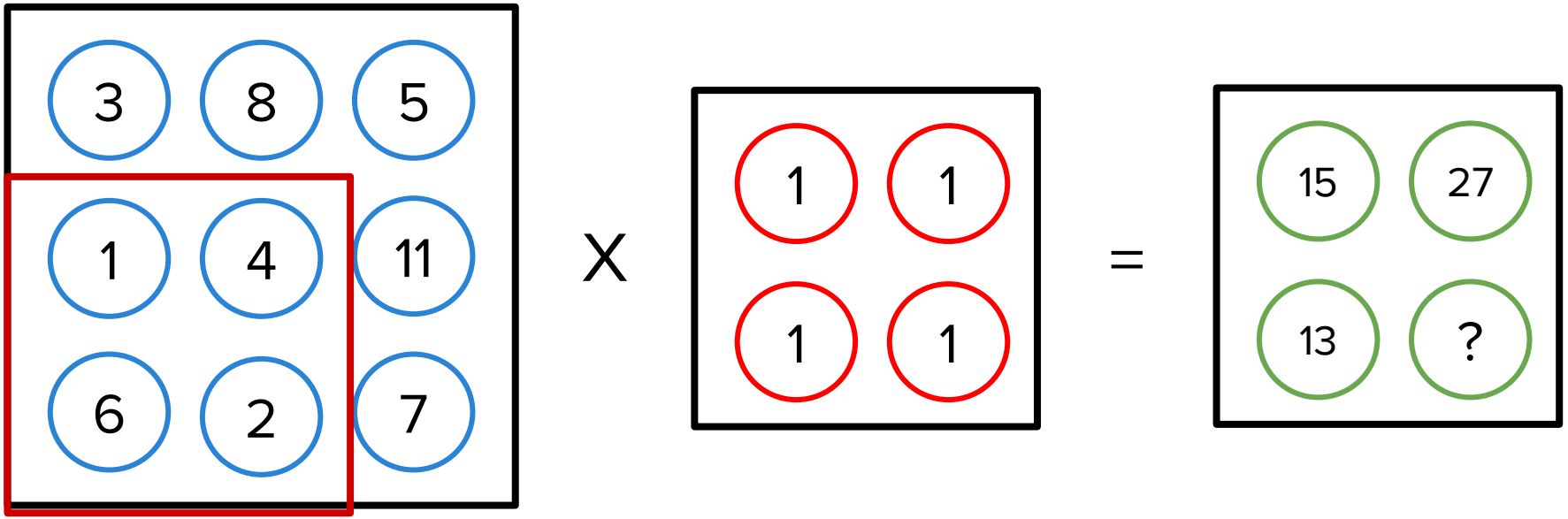
Convolutional Layer



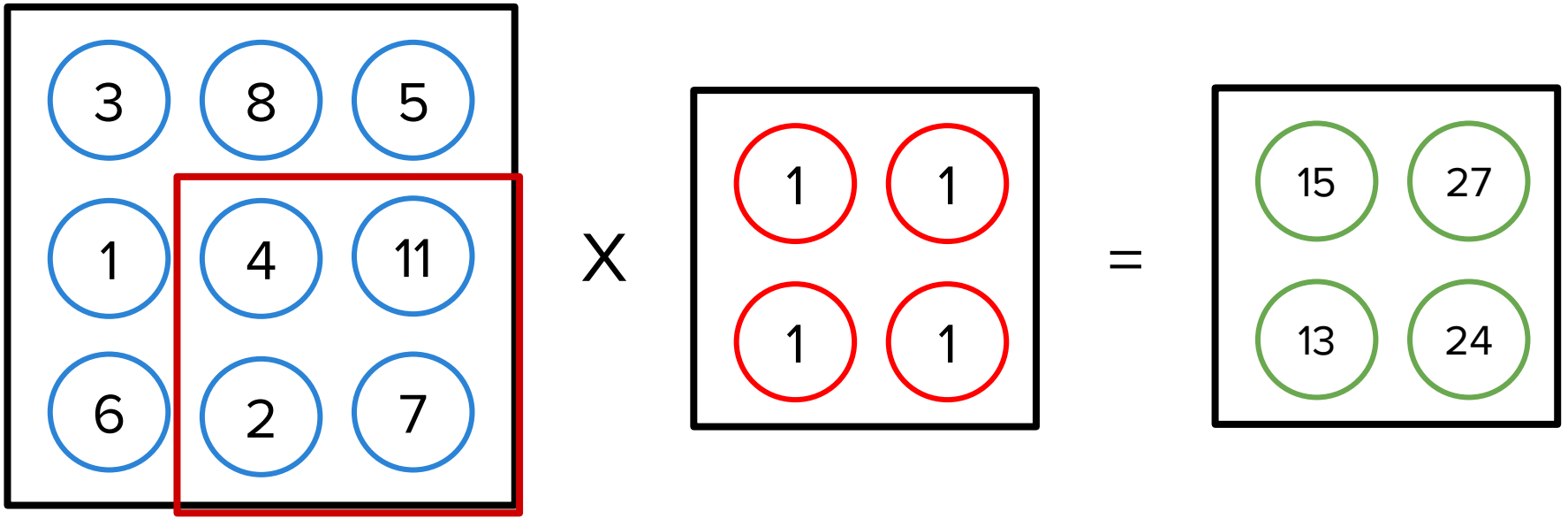
Convolutional Layer



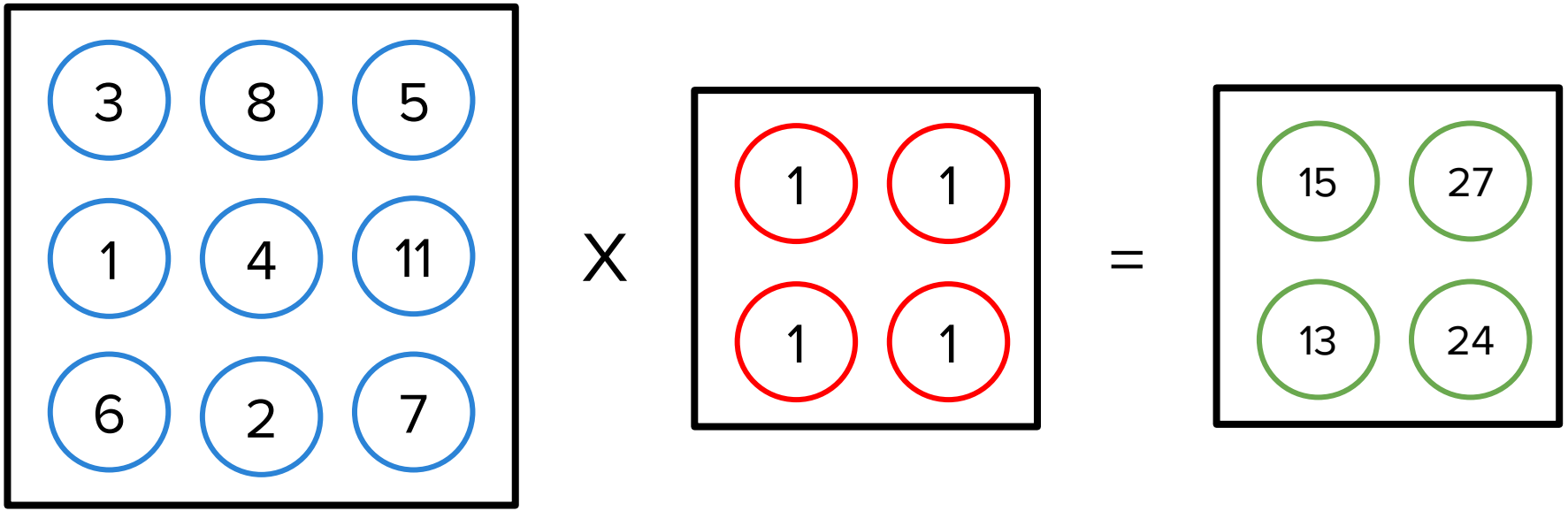
Convolutional Layer



Convolutional Layer

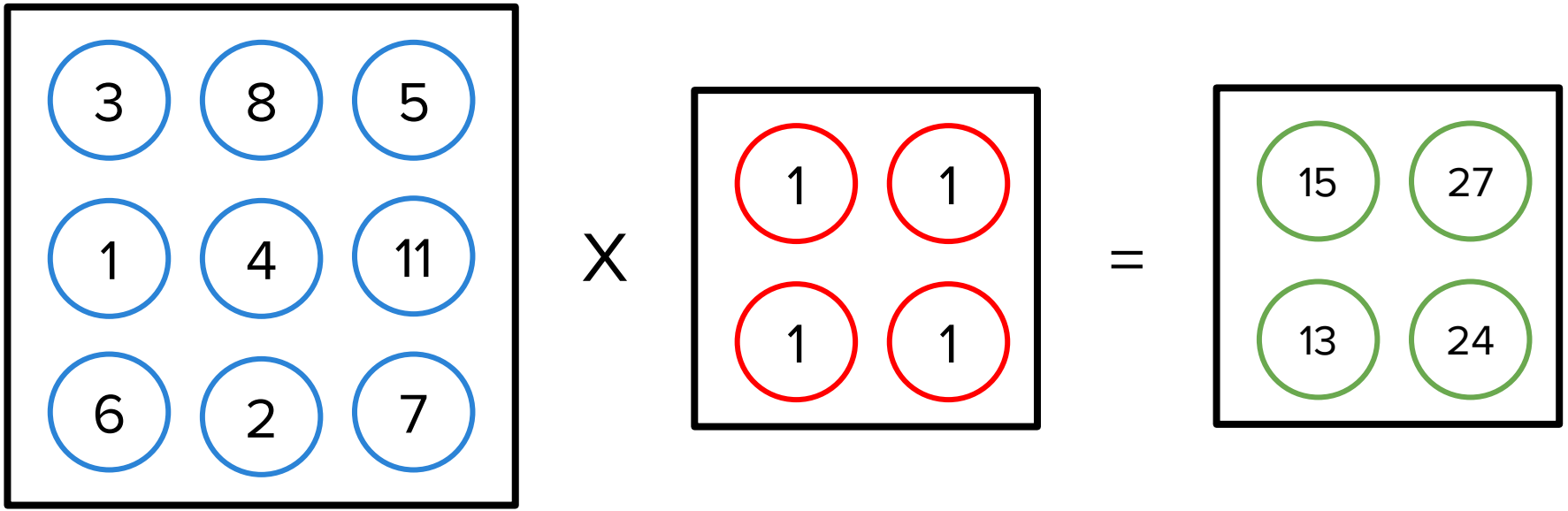


Convolutional Layer

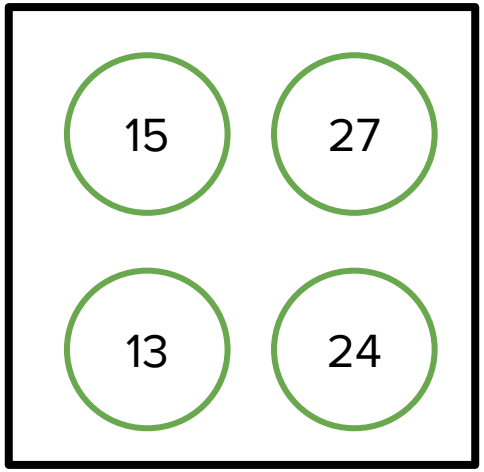


Questions?

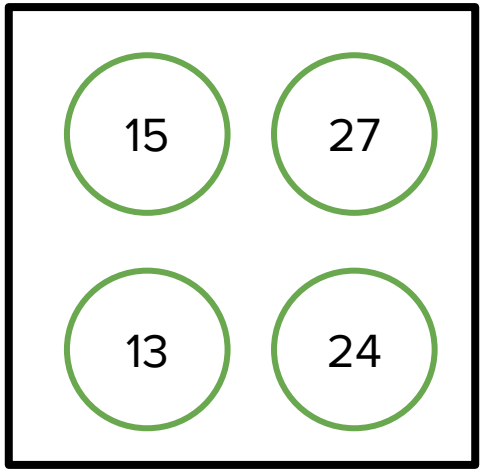
Convolutional Output



Convolutional Output

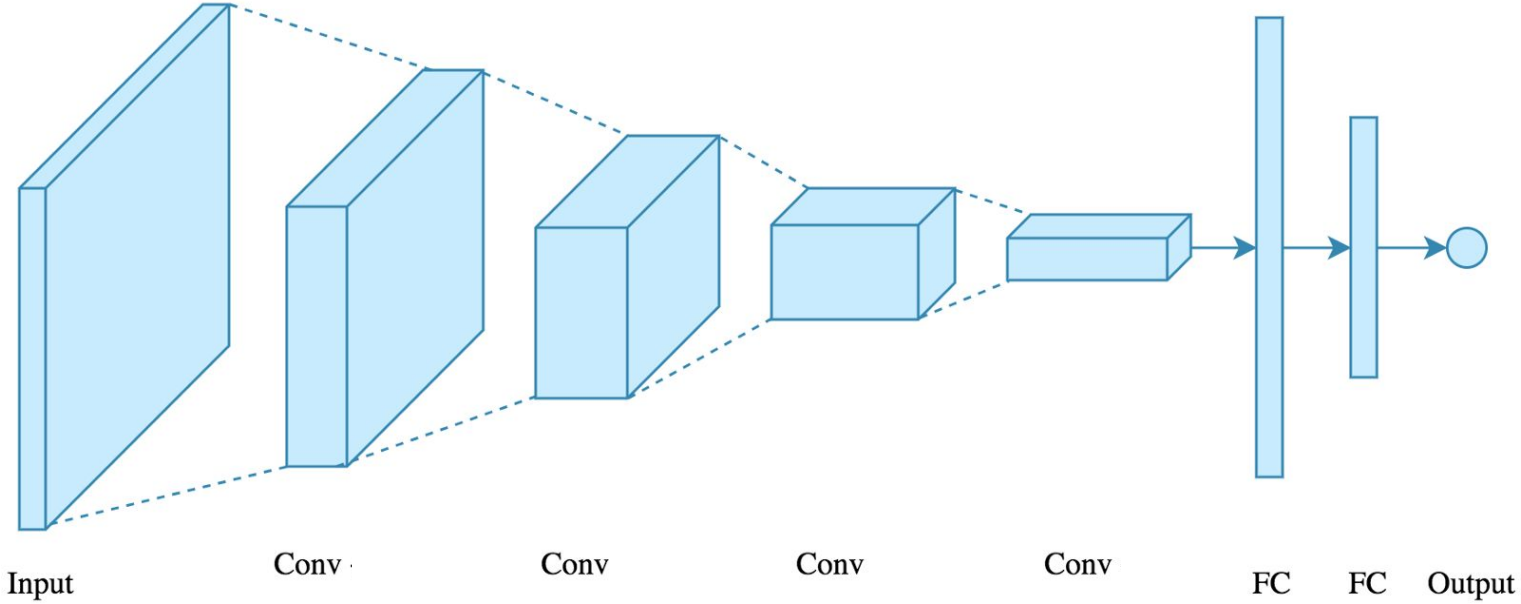


Convolutional Output

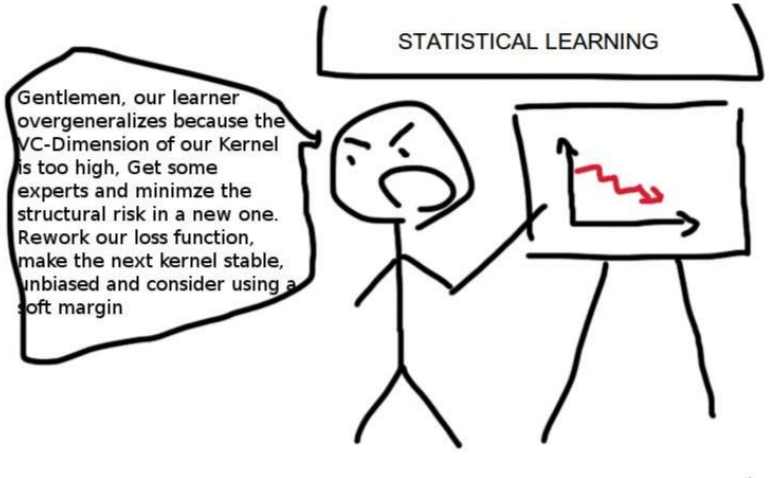


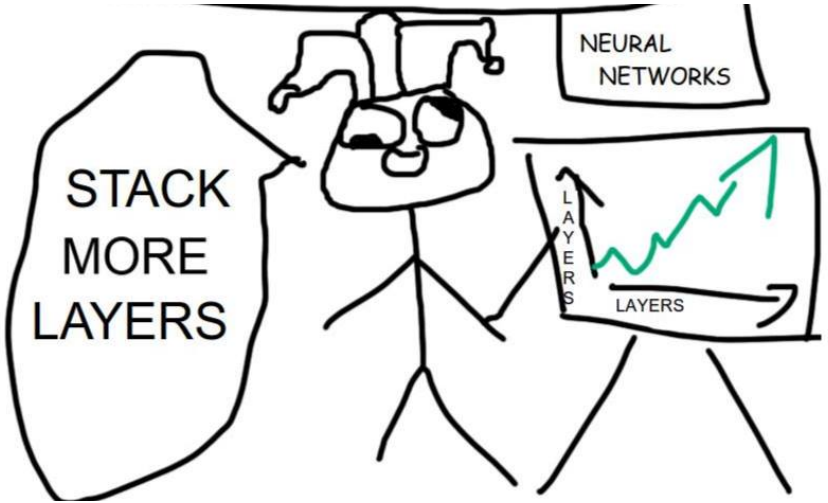
Can be fed as input to another convolutional layer!

Convolutional Neural Network



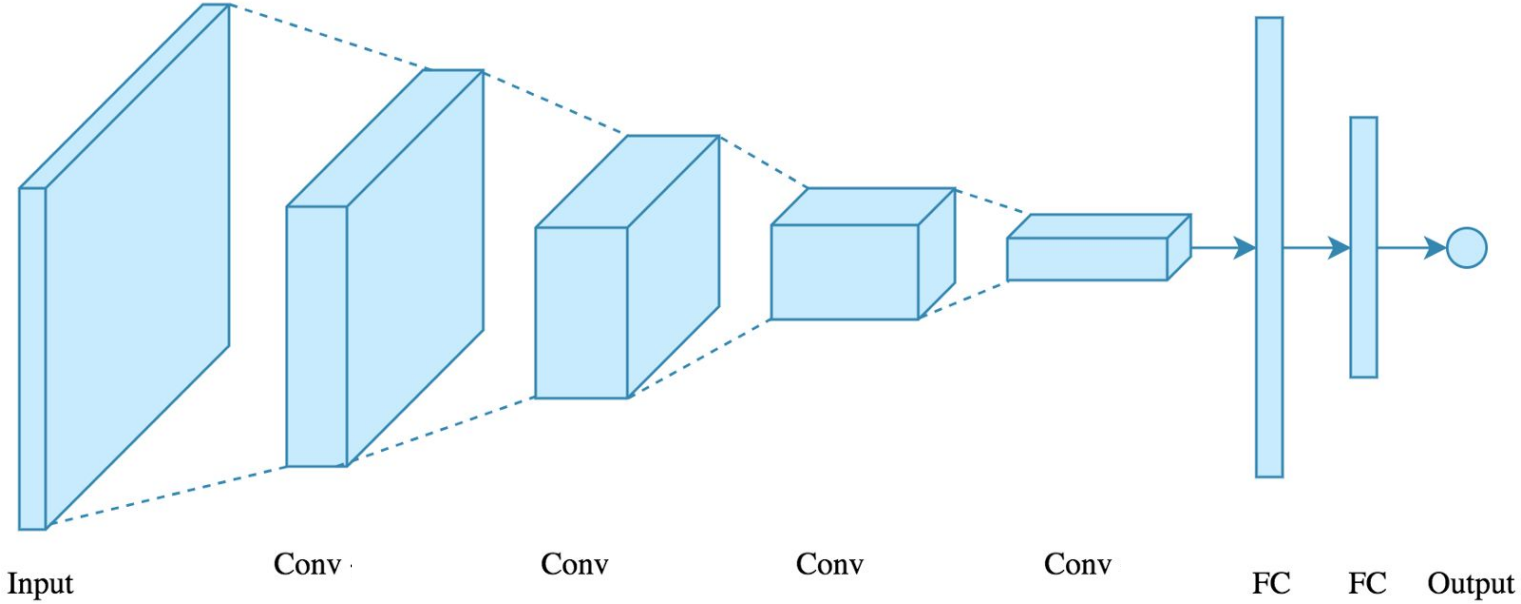
StAcK tHoSe LaYeRs



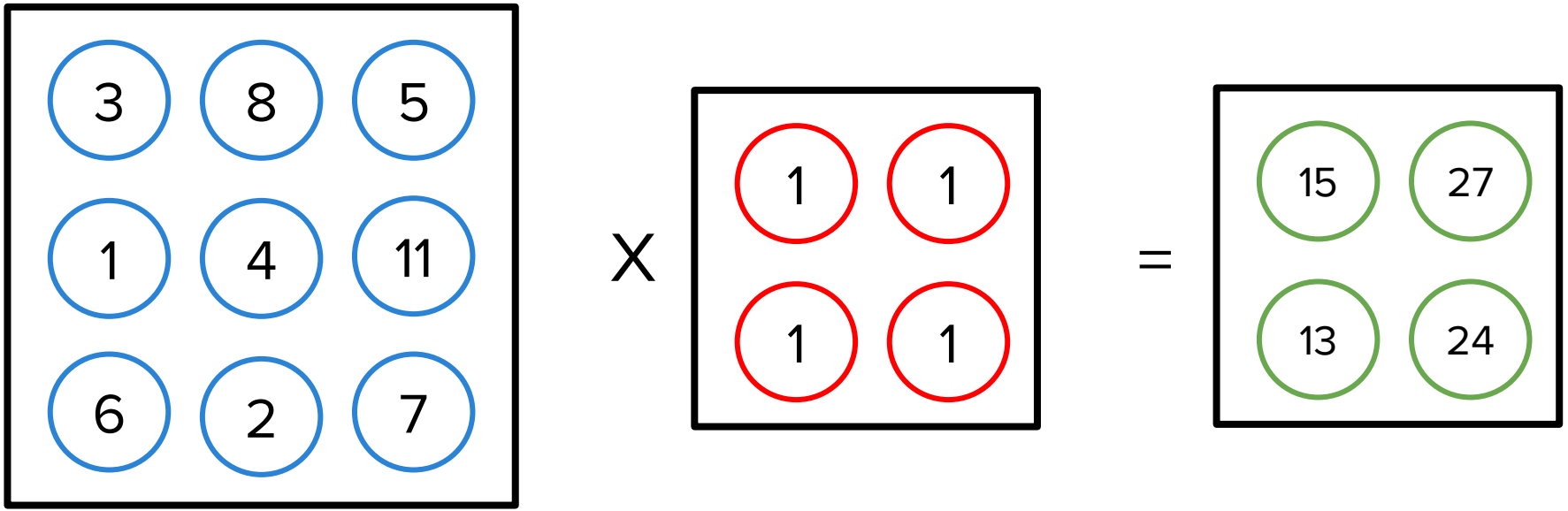


Questions?

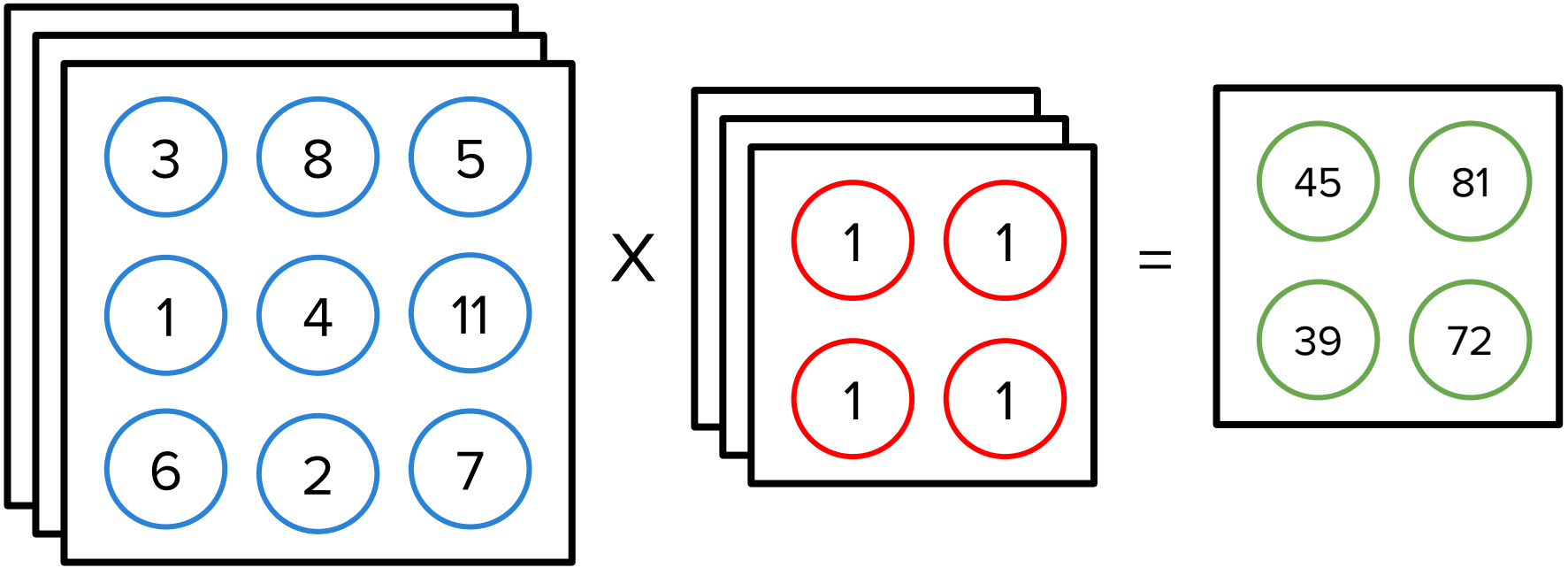
Convolutional Neural Network



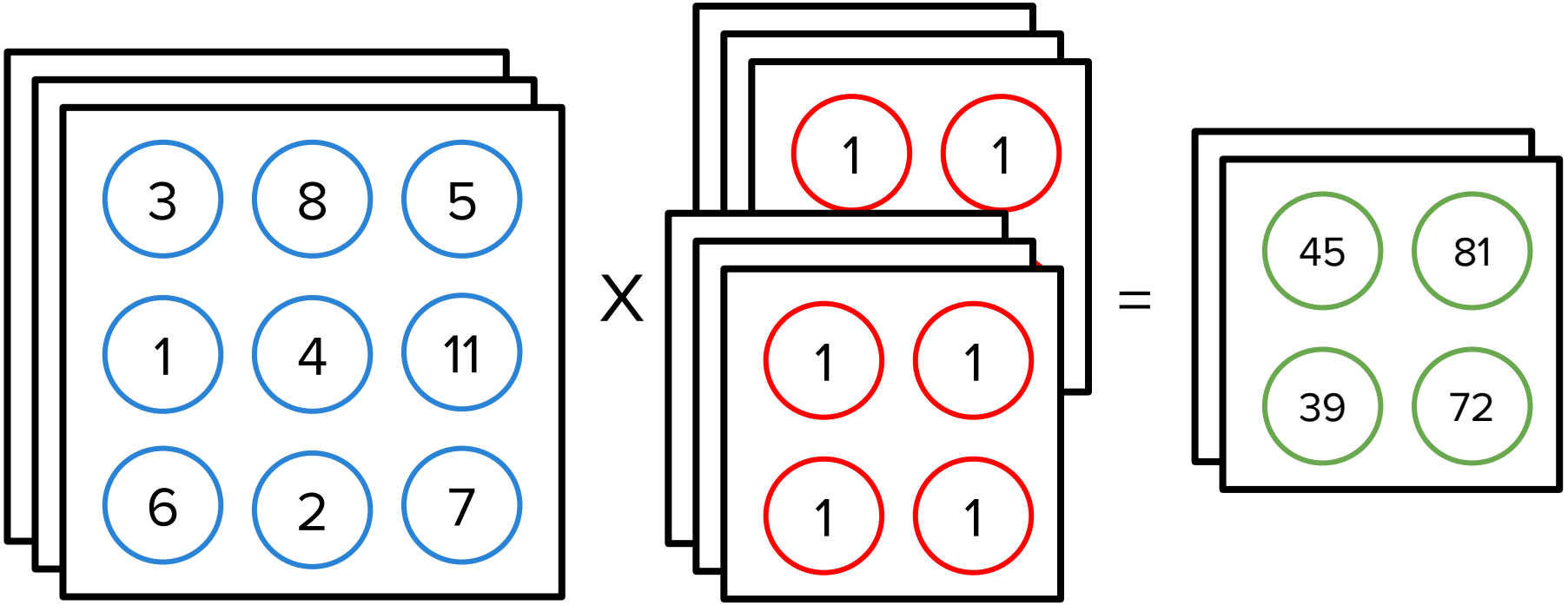
Input/Output Channel Size



Input/Output Channel Size



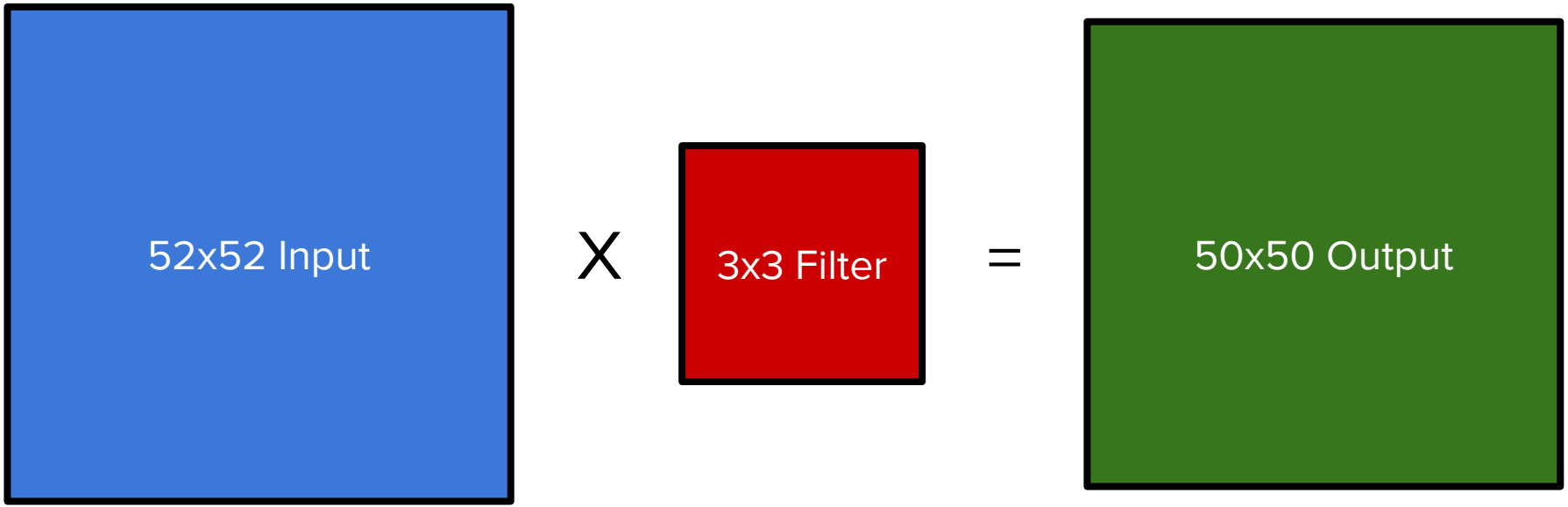
Input/Output Channel Size



Questions?

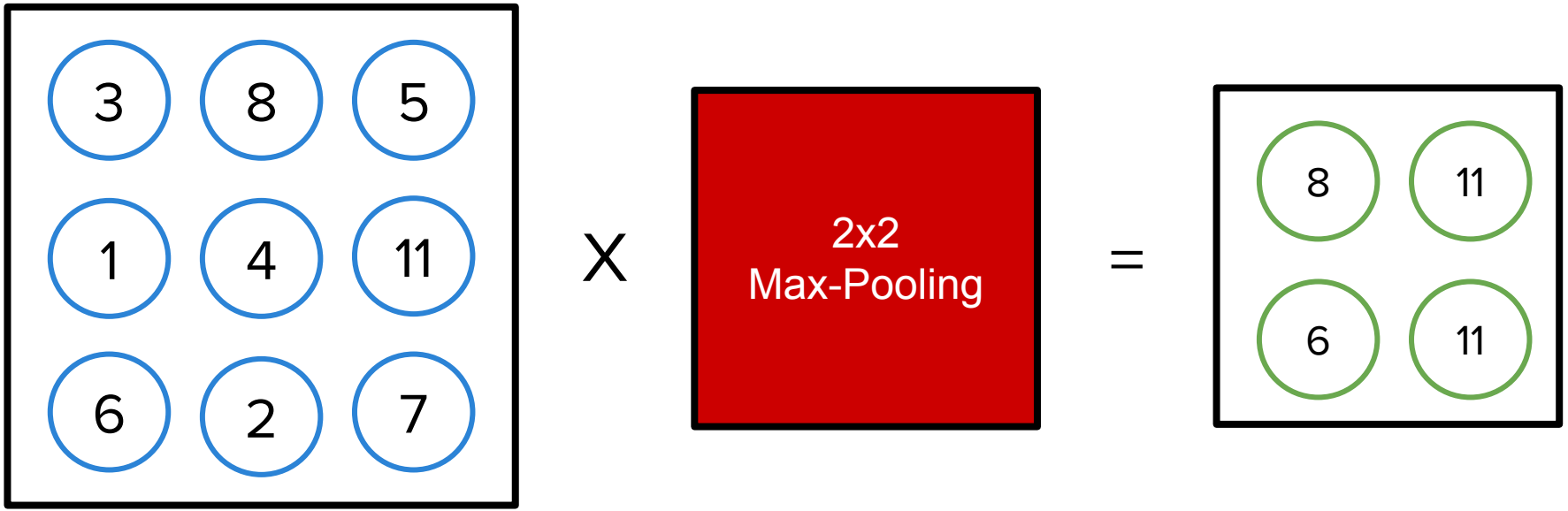
Jupyter Exercises 2: Simple CNN

Problem: Output Size

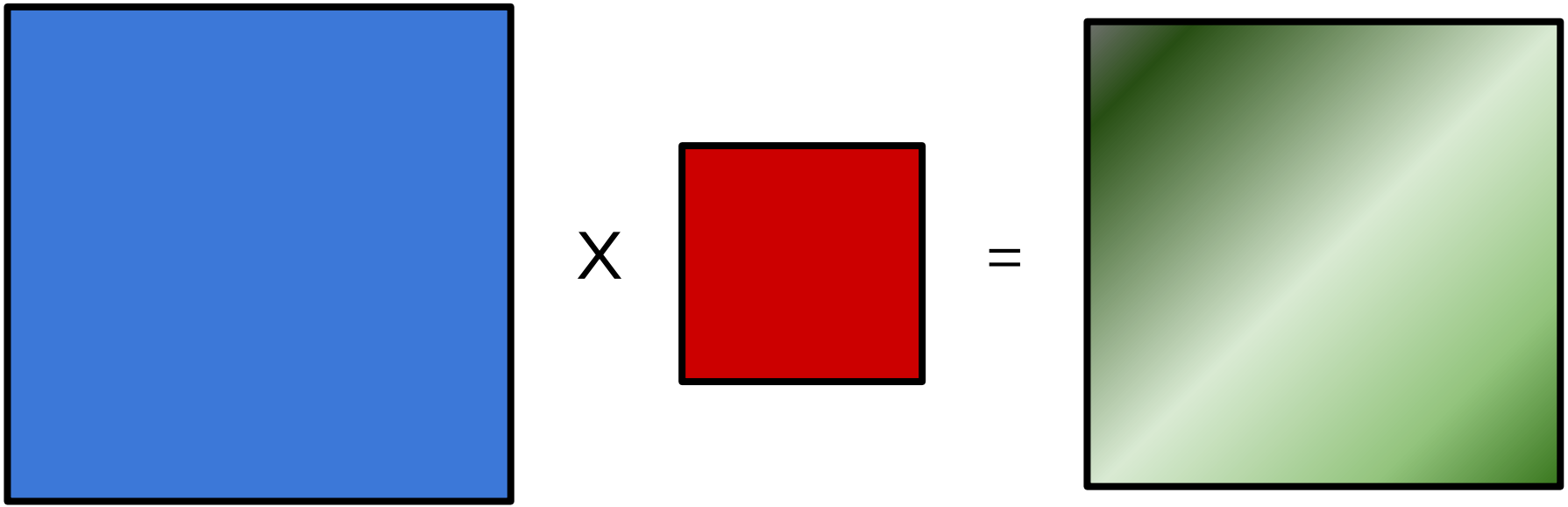


We want to make the output smaller without losing info

Solution: Max-Pooling

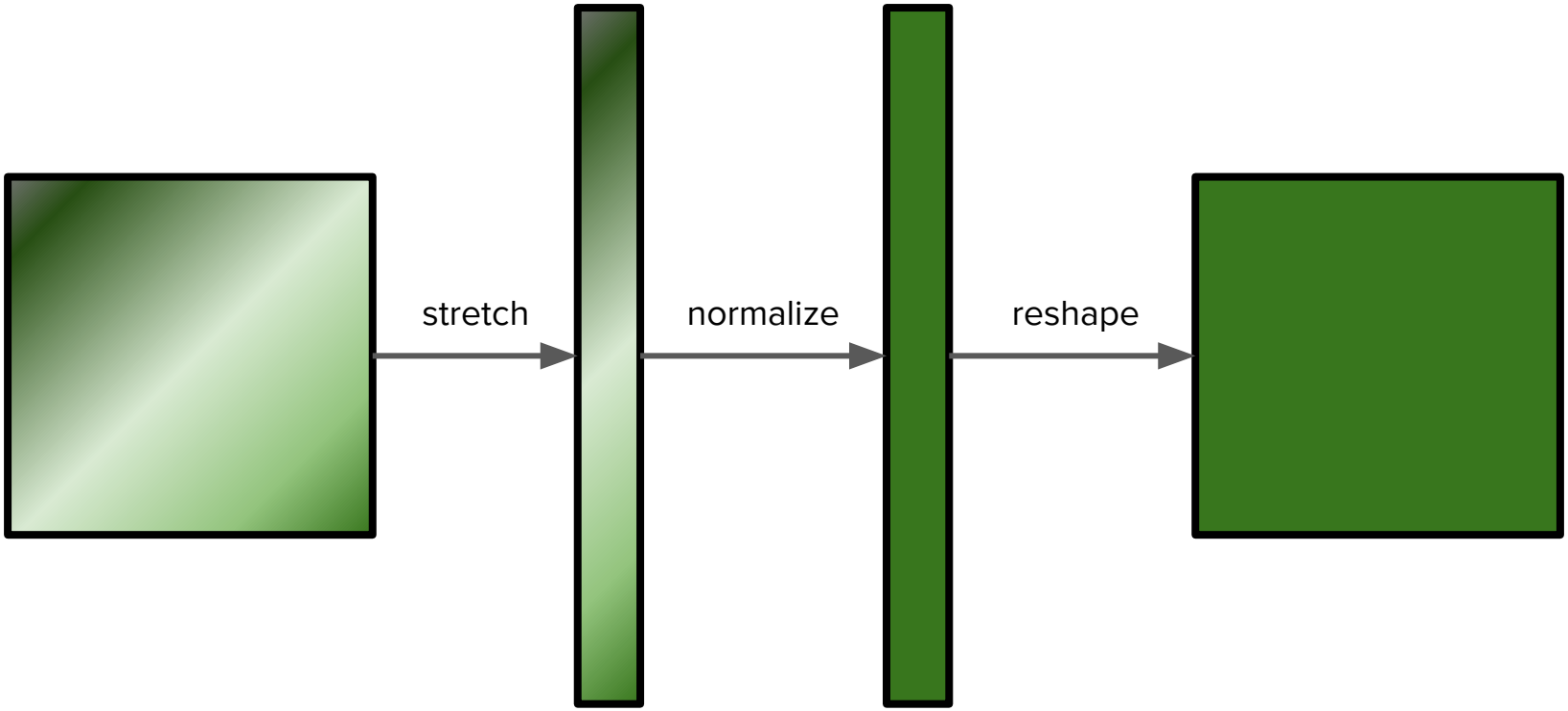


Problem: Covariate Shift



We want to normalize our convolutional output

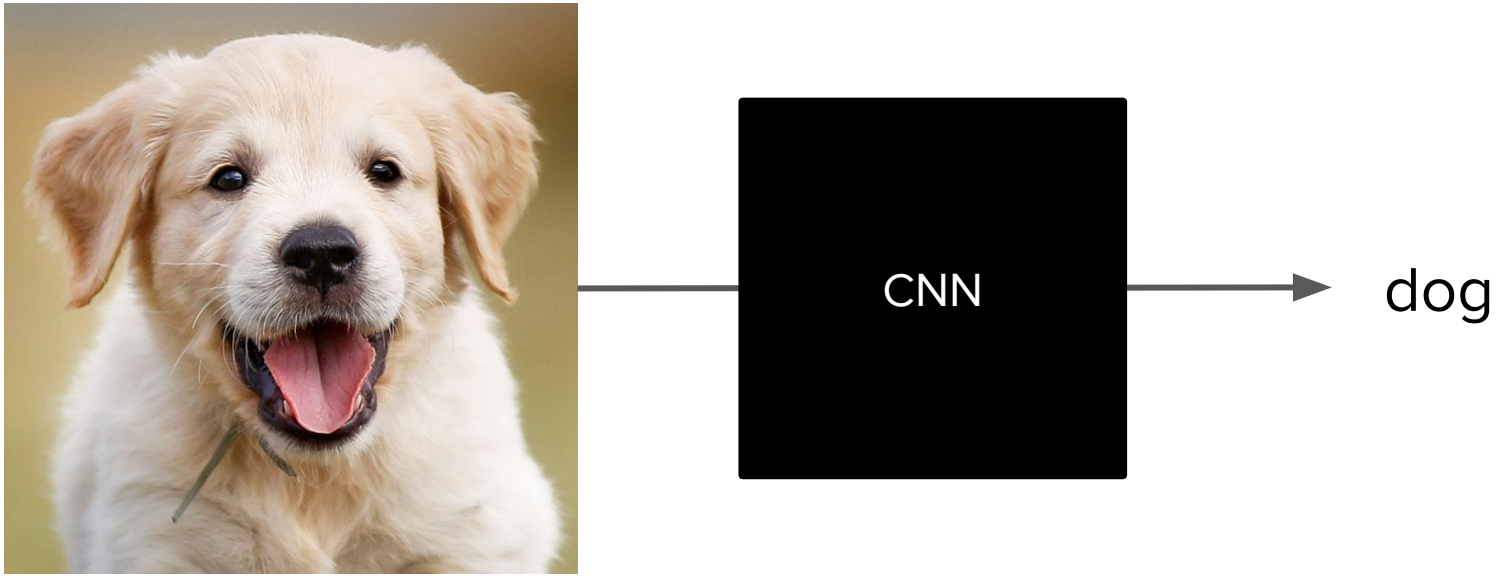
Solution: Spatial Batch Normalization



Questions?

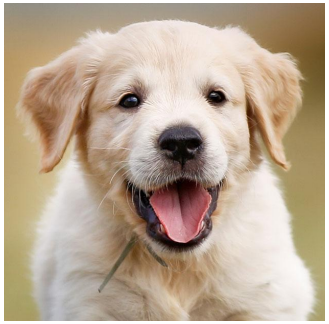
Jupyter Exercises 3: Advanced CNN

Adversarial Attacks



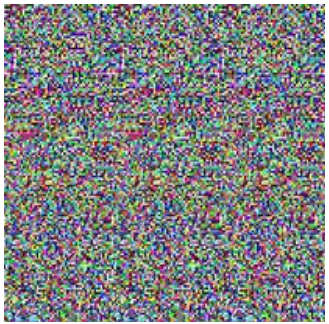
Adversarial Attacks

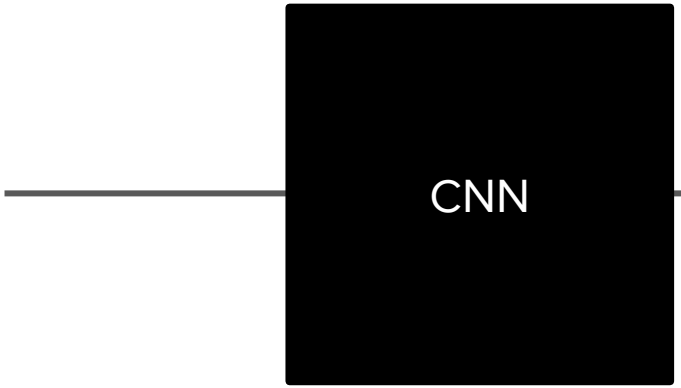
dog



\+

noise

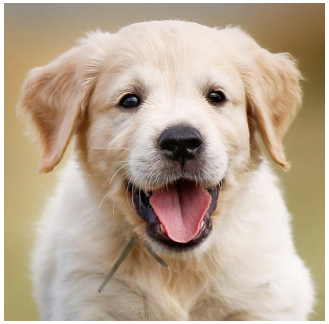




?

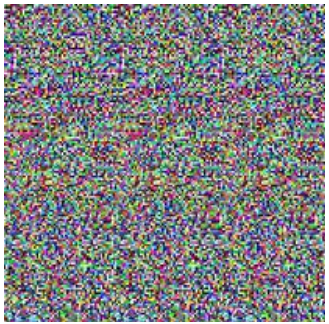
Adversarial Attacks

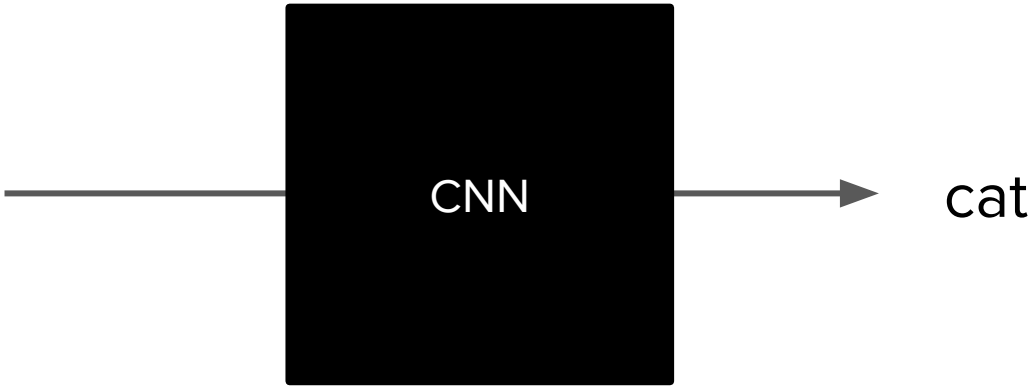
dog



\+

noise





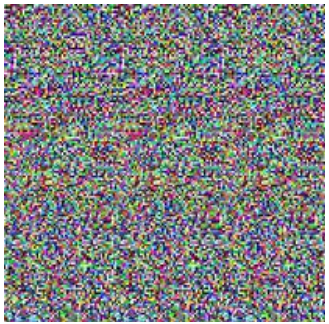
cat

Adversarial Attacks

melanoma

+

noise



CNN for Diagnosis

healthy

Homework: Adversarial Attacks

Summary of Today

- Reviewed of deep neural networks
- Learned about convolutional neural networks
- Implemented CNNs using max-pool and batch-norm
- Learned about adversarial attacks

Questions?