BST 261: Data Science II

Lecture 7

Heather Mattie

Department of Biostatistics
Harvard T.H. Chan School of Public Health
Harvard University

April 9, 2018

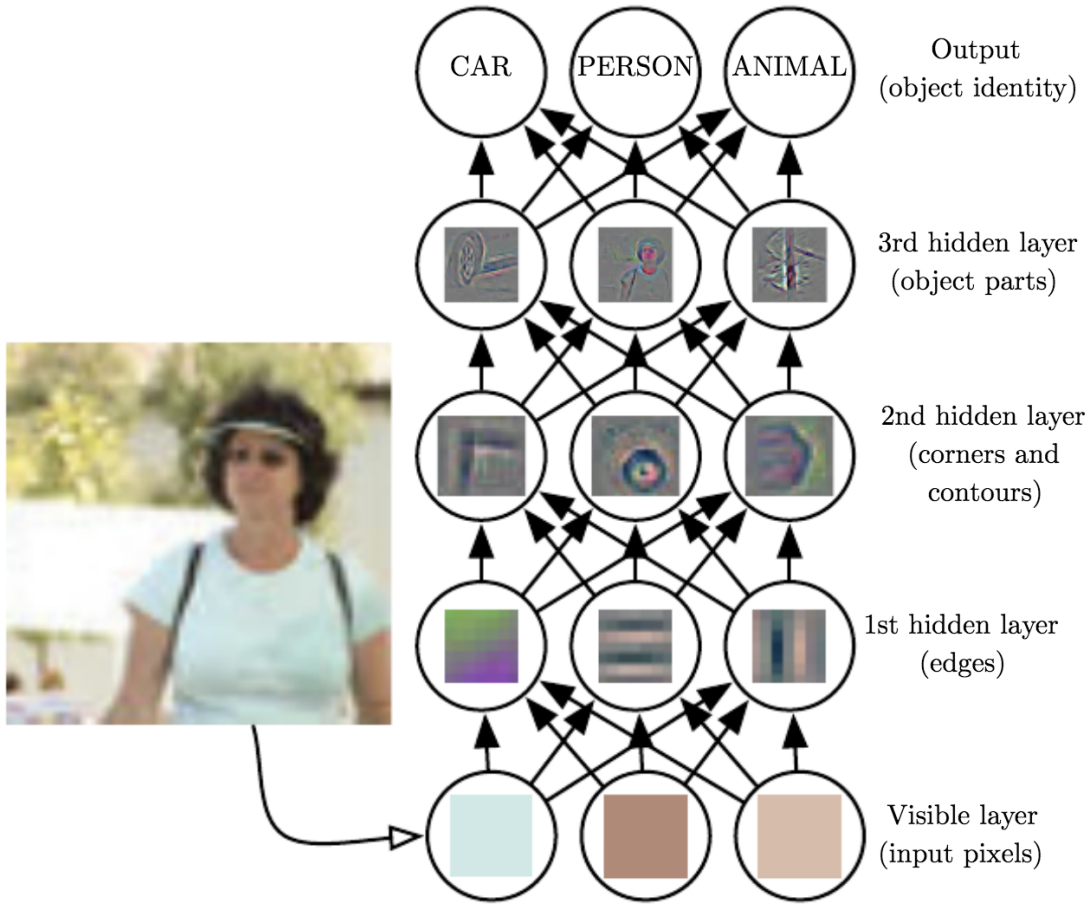
Convolutional Neural Networks (CNNs)

CNNs

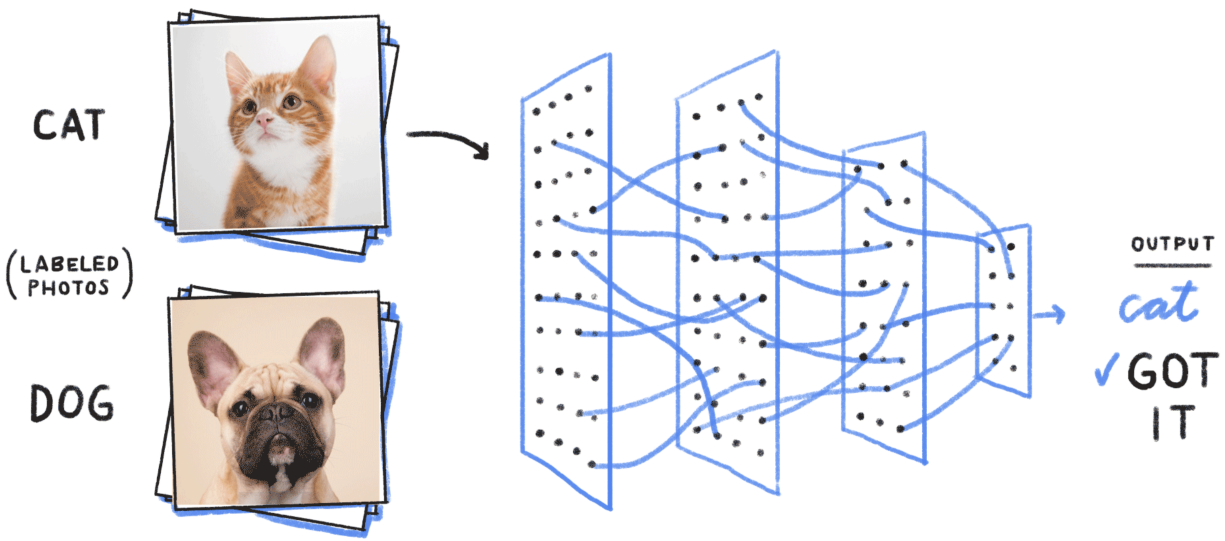
CNNs, or convnets for short, are at the heart of deep learning, emerging in recent years as the most prominent strain of neural networks in research. They have revolutionized computer vision, achieving state-of-the-art results in many fundamental tasks, as well as making strong progress in natural language processing, computer audition, reinforcement learning, and many other areas. CNNs have been widely deployed by tech companies for many of the new services and features we see today. They have numerous and diverse applications, including:

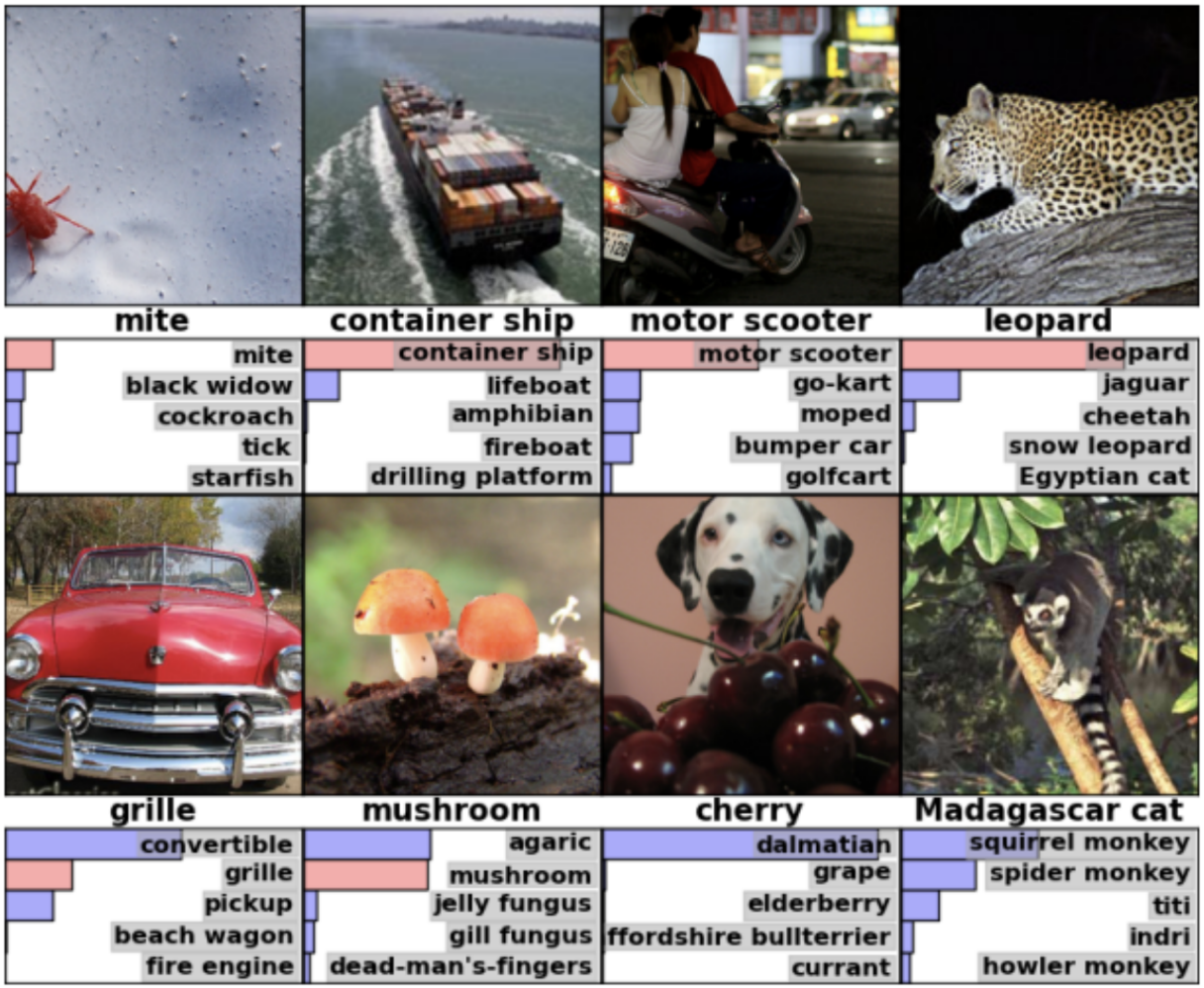
- Detecting and labeling objects, locations, and people in images
- Converting speech into text and synthesizing audio of natural sounds
- Describing images and videos with natural language
- Tracking roads and navigating around obstacles in autonomous vehicles
- Analyzing videogame screens to guide autonomous agents playing them
- “Hallucinatin” images, sounds, and text with generative models

Computer Vision



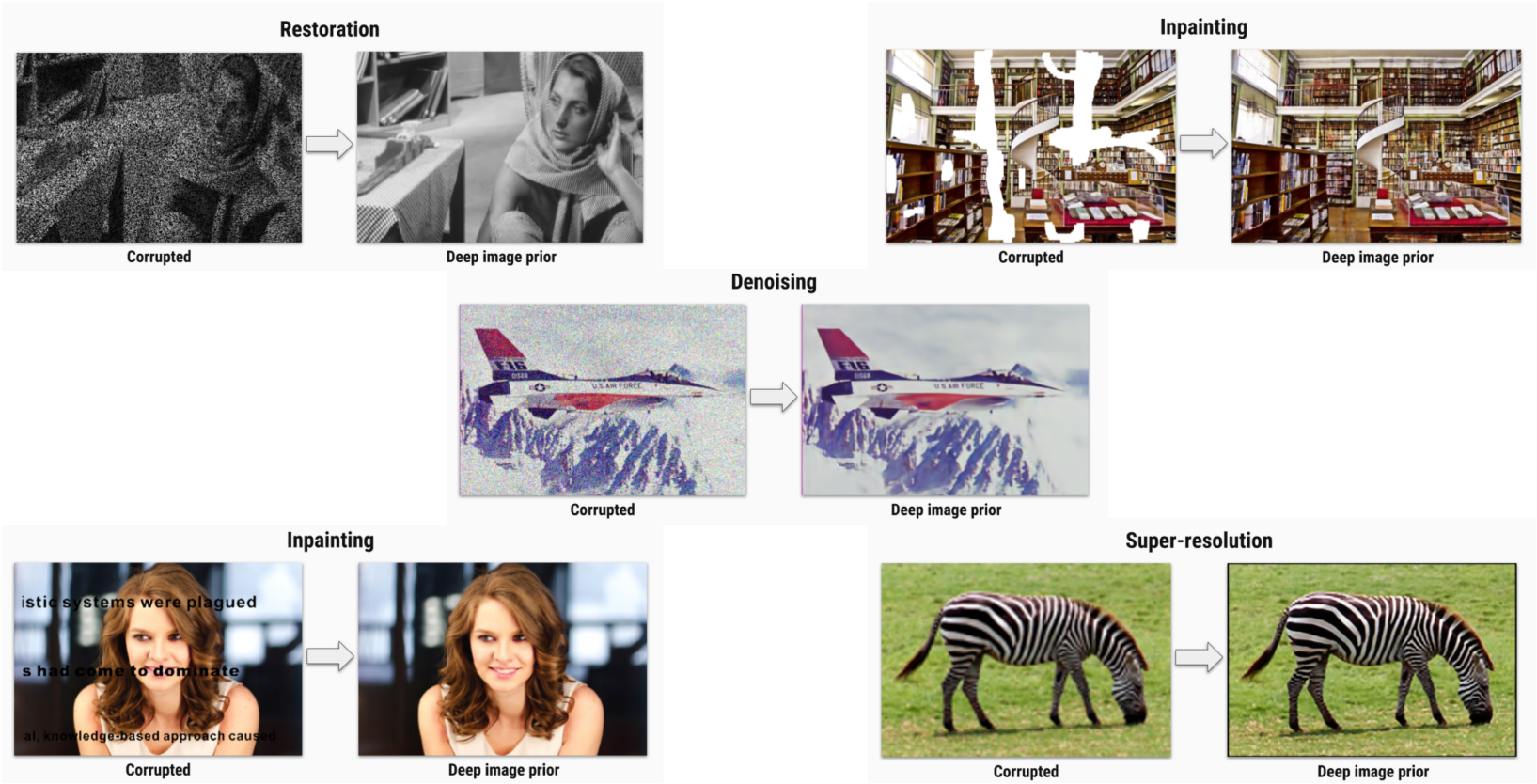
Computer Vision





Top: 4 correctly classified examples. Bottom: 4 incorrectly classified examples. Each example has an image, followed by its label, followed by the top 5 guesses with probabilities. From Krizehvsky *et al.* (2012).

Restoration, Inpainting, Denoising and Super-resolution



Autonomous Cars

- YouTube video: `https://www.youtube.com/watch?v=bDOnn0-4Nq8`

MNIST Example

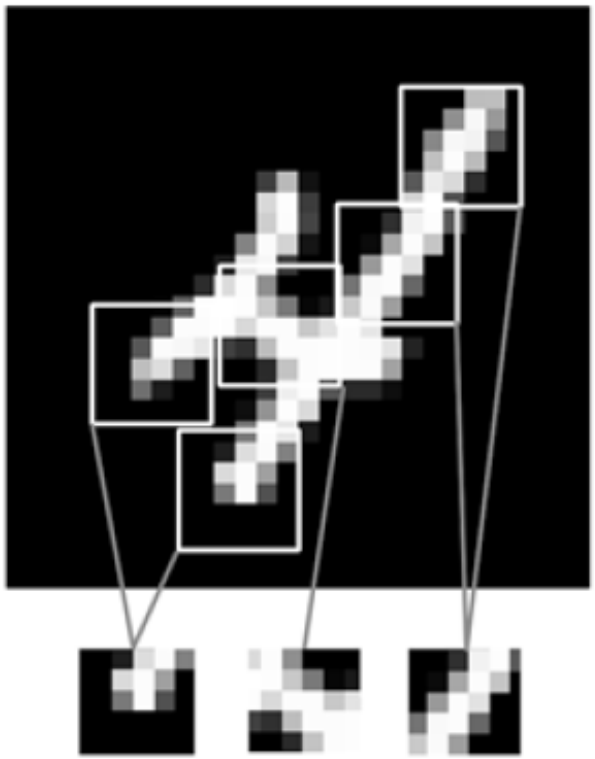
```
import keras
from keras import layers
from keras import models
from keras.datasets import mnist
from keras.utils import to_categorical

(train_images, train_labels), (test_images, test_labels) = mnist.load_data()

train_images = train_images.reshape((60000, 28, 28, 1))
train_images = train_images.astype('float32') / 255

test_images = test_images.reshape((10000, 28, 28, 1))
test_images = test_images.astype('float32') / 255

train_labels = to_categorical(train_labels)
test_labels = to_categorical(test_labels)
```

MNIST Example

```
model = models.Sequential()
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape=(28, 28, 1)))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))

model.add(layers.Flatten())
model.add(layers.Dense(64, activation='relu'))
model.add(layers.Dense(10, activation='softmax'))

model.compile(optimizer='rmsprop',
              loss='categorical_crossentropy',
              metrics=['accuracy'])
model.fit(train_images, train_labels, epochs=5, batch_size=64)
```

CNNs vs Deep Feedforward Networks

- The fundamental difference between the feedforward networks we've seen and CNNs, is that dense layers learn **global** patterns while convolution layers learn **local** patterns



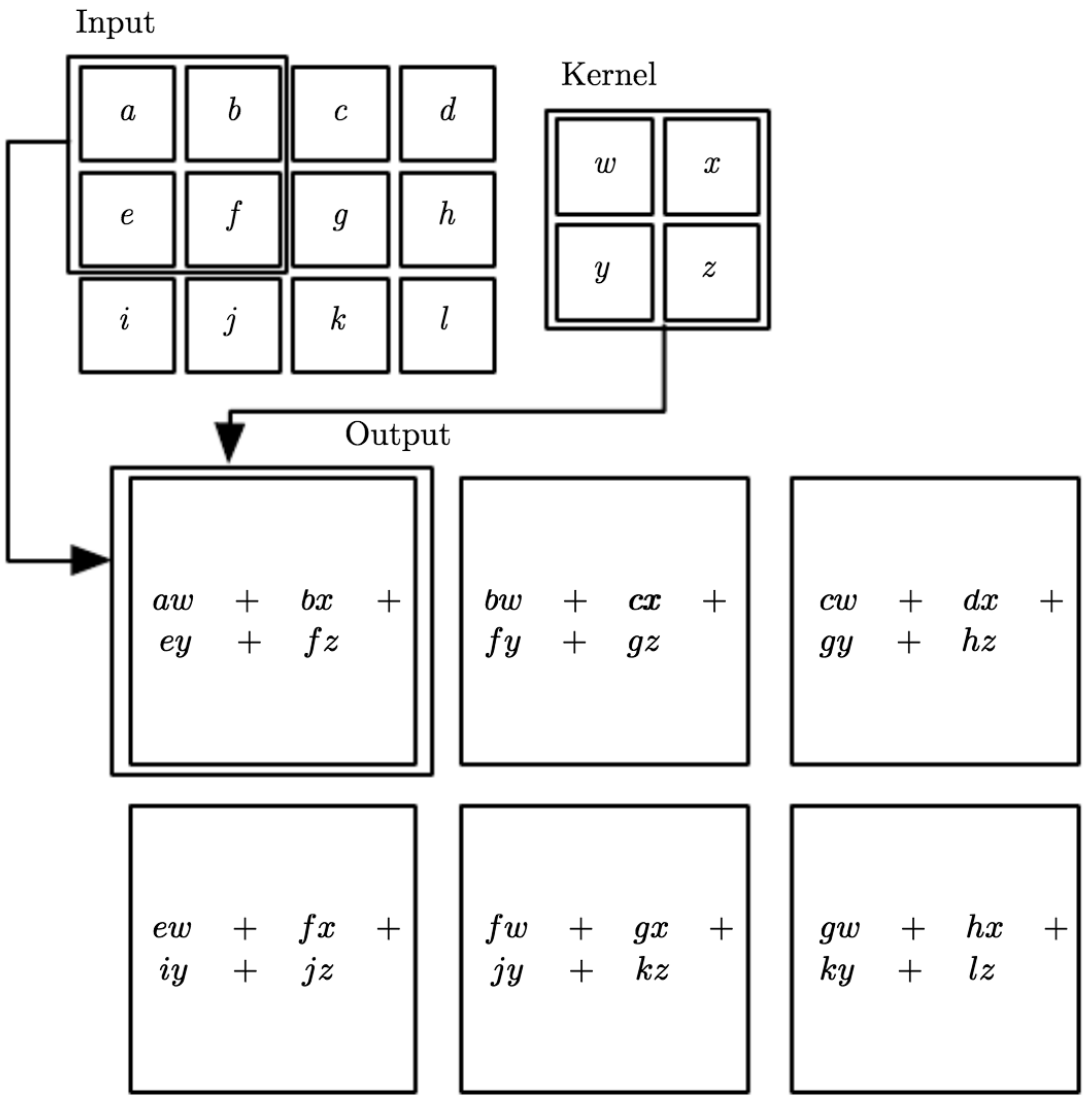
The Convolution Operation

- The primary purpose of the convolution operation is to extract features from the input
- To do this, the input is split into several different areas, and the convolution operation applied to each area
- A summary value is then calculated and kept as part of the output
- Here, I is the $n \times m$ input image (sometimes called **feature map**), K is a two-dimensional **kernel**, or more commonly, **filter**, and is a weighting function
- The output resulting from this operation is called the **response map**

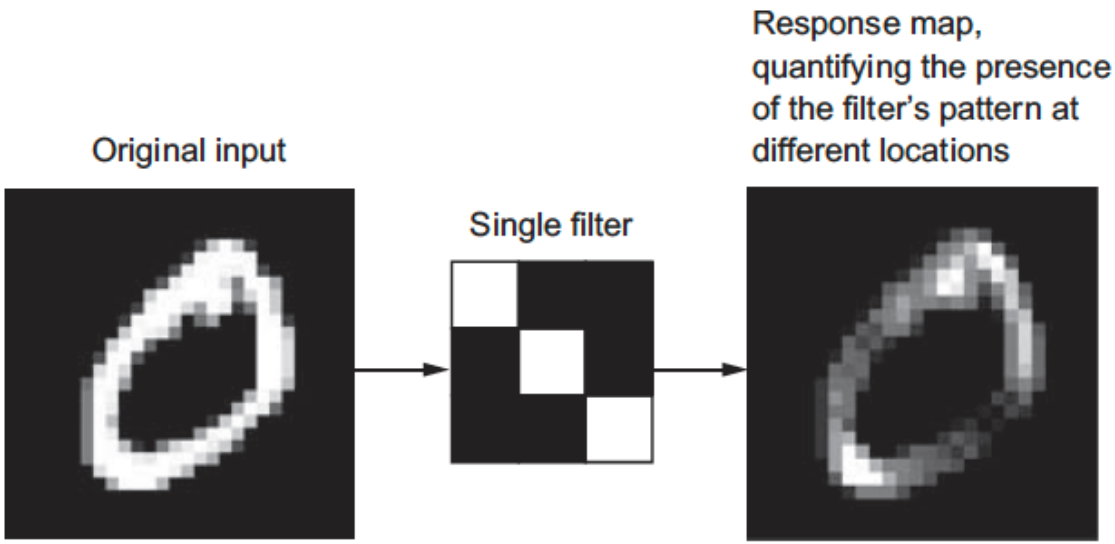
$$S(i,j) = (I * K)(i,j) = \sum_m \sum_n I(m,n)K(i-m, j-n) \tag{1}$$

- Note: some neural networks implement a related function called the **cross-correlation**, but call it convolution. They are very similar and in some instances equivalent

The Convolution Operation



The Convolution Operation



Filters

- The most common filter sizes are 3×3 and 5×5
- Sometimes 7×7 filters are also used
- A 1×1 filter is a special case that we will see later in the course
- Odd dimension filters are preferred for computer vision
  - Natural padding (we'll see that in the following slides)
  - Ensures a 'central' position or pixel of the filter

Motivation

Convolution leverages 3 important ideas that can help improve a machine learning system:

- **Sparse interactions** / sparse connectivity / sparse weights
  - Filters are smaller than the input images and thus fewer parameters (weights) need to be stored
  - This reduces computational expense and improves statistical efficiency
- **Parameter sharing**
  - The same parameter is used for more than one function in the model
  - In a CNN, each each element of the filter is applied to every position of the input
- **Equivariant representations**
  - Parameter sharing causes equivariance to translation: if the input changes, the output changes in the same way
  - A function $f(x)$ is invariant to a function g if $f(g(x)) = g(f(x))$
  - When processing time-series data, this means that convolution produces a sort of timeline that shows when different features appear in the input
  - Note that convolution is not equivariant to some other transformations, such as changes in the scale or rotation of an image
- Translation invariant: After learning a certain pattern from one part of an image, it can recognize it anywhere
- Convolution also provides a way to work with inputs of different size

- Example of both sparse interactions and parameter sharing:

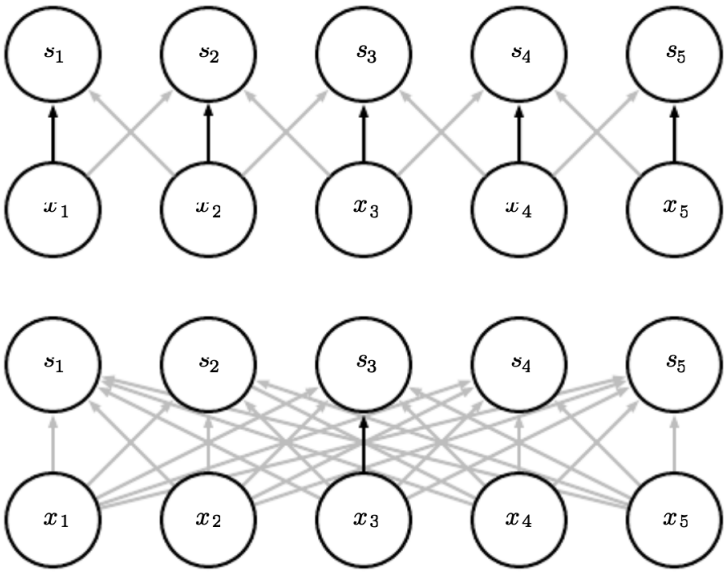
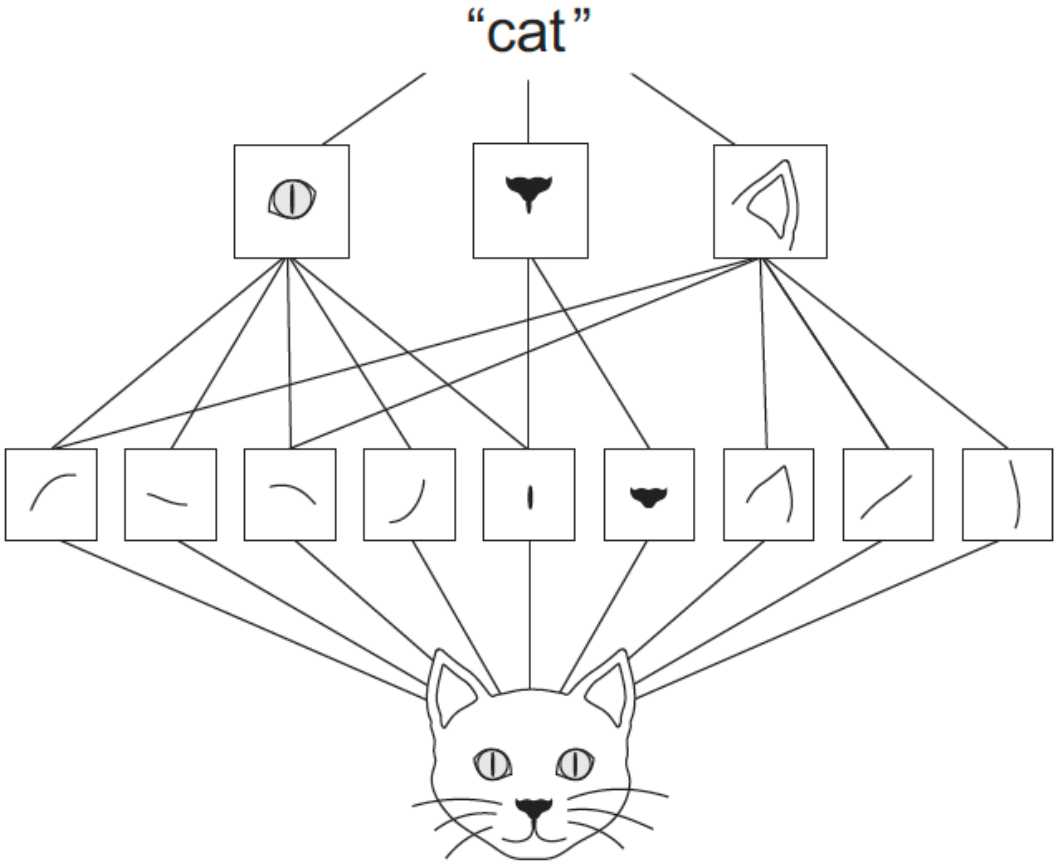


Figure 9.5: Parameter sharing. Black arrows indicate the connections that use a particular parameter in two different models. *(Top)*The black arrows indicate uses of the central element of a 3-element kernel in a convolutional model. Because of parameter sharing, this single parameter is used at all input locations. *(Bottom)*The single black arrow indicates the use of the central element of the weight matrix in a fully connected model. This model has no parameter sharing, so the parameter is used only once.

Motivation

- CNNs learn **spacial hierarchies** of patterns: one convolutional layer will learn small patterns and the next larger patterns made of the features of the layer before, and so on

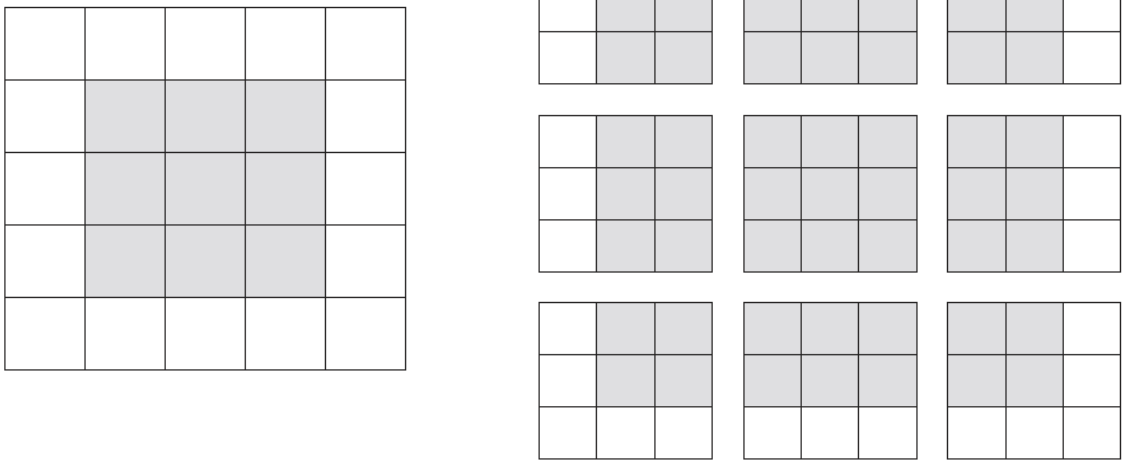


Padding

- Applying a filter to an input image shrinks it - the output dimensions are smaller than the input dimensions
- Additionally, when we perform the convolution operation on an input, the pixels on the edges aren't used as much as the pixels in the middle
- To make the amount of information used more equal across pixels, you can use **padding**
- Padding consists of adding an appropriate number of rows and columns to each side of the image (think a border of pixels)
- This enables an output with the same dimensions as the input

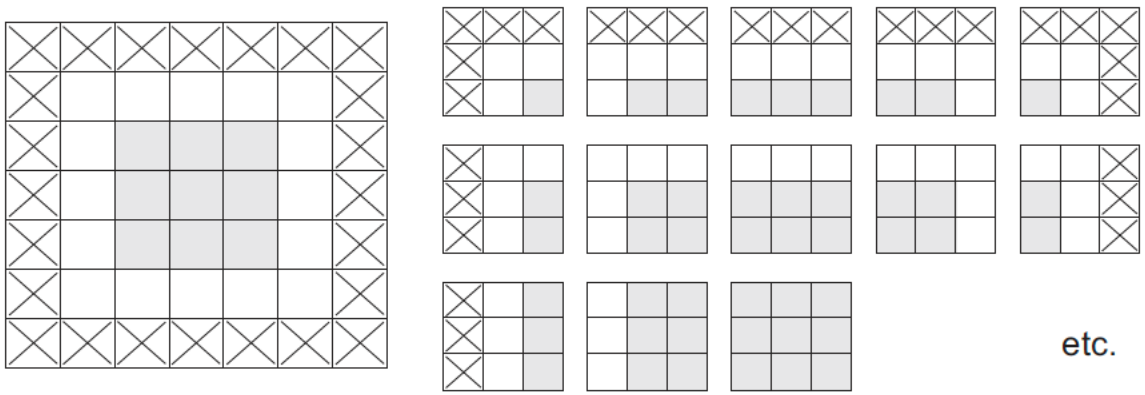
Valid Padding

- In Keras, the default is no padding, or **'valid' padding**
- This means the output will not be the same dimension as the input, and will instead depend on the dimension of the input and the size of the filter
- Below is a 5×5 image
- If we apply a 3×3 filter, the output will also be 3×3



Same Padding

- Below is the same 5×5 image, but with an added border
- If we use a 3×3 filter, we need to add $p = 1$ padding - here, p is the number of rows to add to the border of an image
- The output will then be 5×5
- Because the input and output have the same dimensions, this is called **'same' padding**



General Padding Formula

- There is a general formula that can help you decide how much padding you need or want
- Let the input be $n \times m$ and the filter $f \times f$
- Without padding, the output would be:

$$(n - f + 1) \times (n - f + 1) \tag{2}$$

- For an output with the same dimension as the input, need p such that:

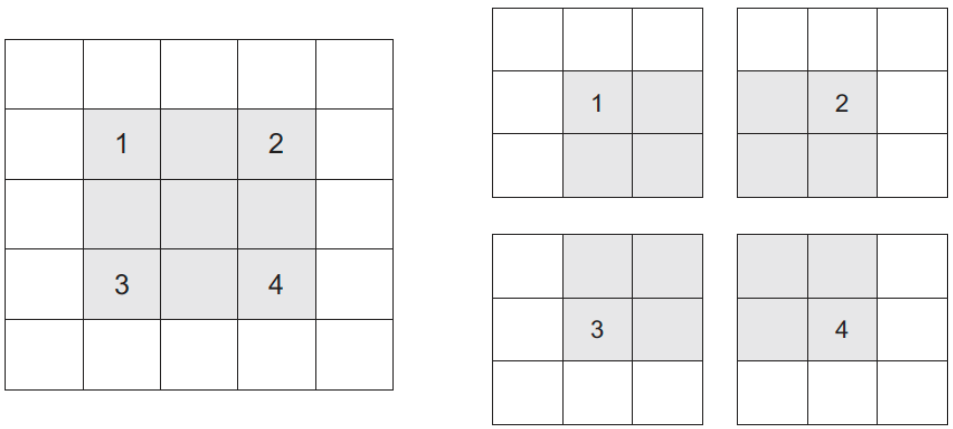
$$n \times m = (n + 2p - f + 1) \times (m + 2p - f + 1) \tag{3}$$

- Which boils down to $p = \frac{f-1}{2}$

Convolution Strides

- Another factor that can influence output size is convolution **strides**
- So far we have assumed that we slide our filter over a single space to extract a new patch - but what if we wanted to slide over 2 spaces, 3 spaces, or more?
- Convolutional strides are convolutions with a stride greater than 1
- If your stride is set equal to 2, you will downsample the width and height of the input image by a factor of 2
- If s is the size of the stride, the output will have dimensions

$$\left\lfloor \frac{n + 2p - f}{s} + 1 \right\rfloor \times \left\lfloor \frac{m + 2p - f}{s} + 1 \right\rfloor \tag{4}$$

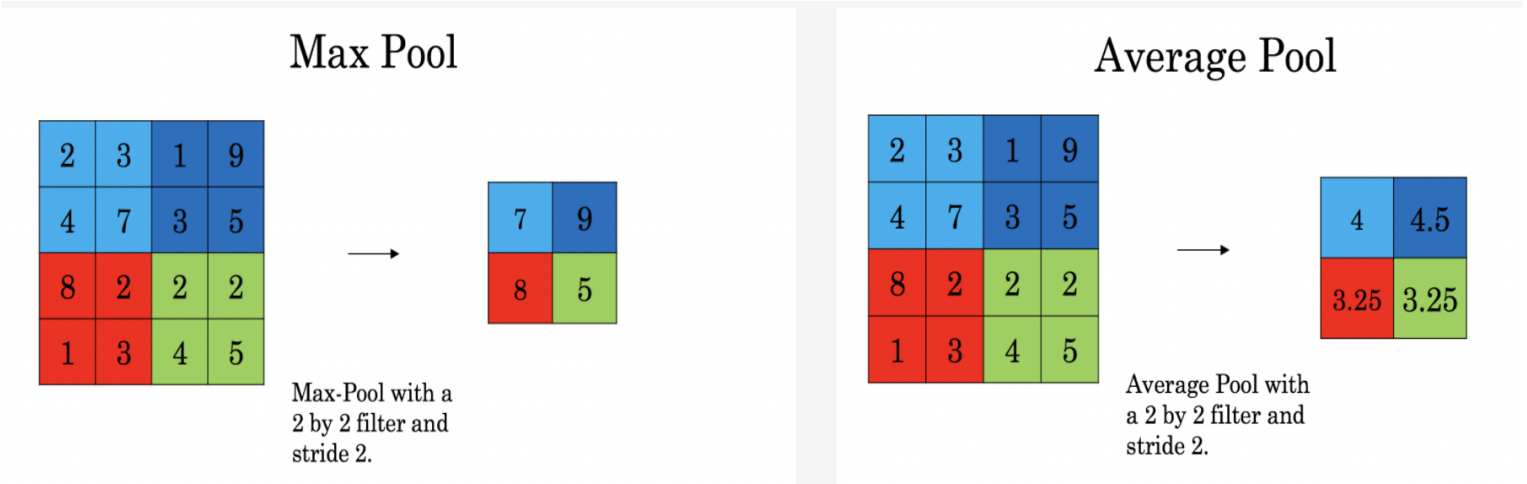


- Strided convolutions are rarely used in practice - **max-pooling** is more common

Pooling

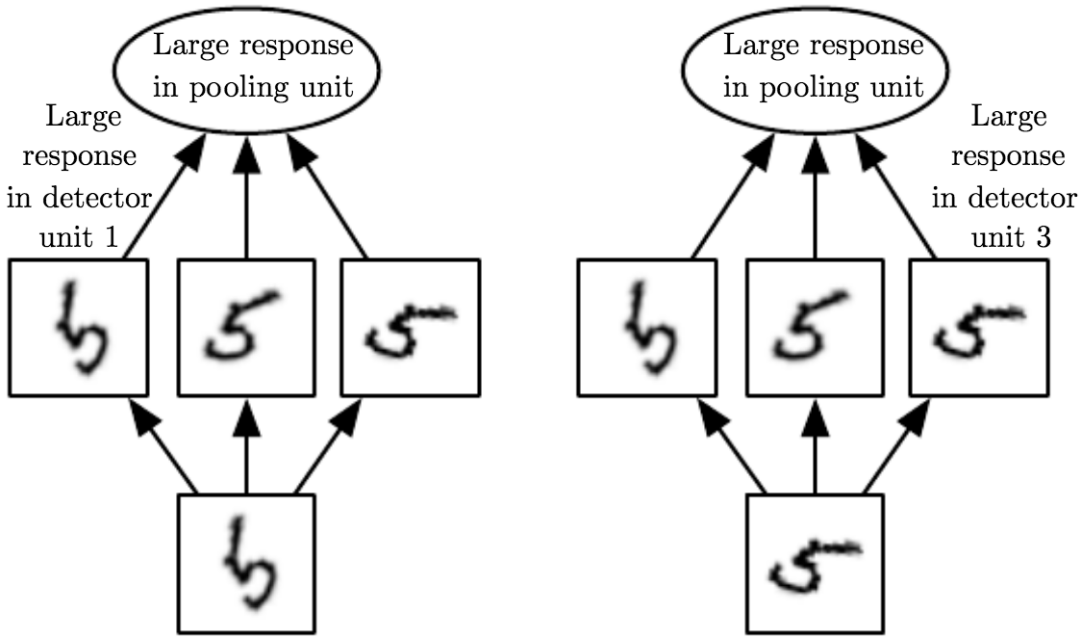
- A typical layer of a CNN consists of 3 stages:
  - Convolution stage - linear transformation of the input
  - Detector stage - Nonlinear activation (ex: `relu` activation function is applied)
  - Pooling stage - further modification (downsizing) of the output
- A pooling function replaces the output at a certain location with a **summary statistic** of the nearby outputs
- Pooling greatly reduces the computational expense of the network by decreasing the number of parameters to be learned
- There are different types of pooling
  - Max pooling
    - Outputs the maximum value from a patch for each channel
    - Similar to convolution, but instead of transforming patches via a learned linear transformation, they're transformed via a hardcoded `max` tensor operation
    - Very common
    - Usually done with 2×2 windows
  - Average pooling
  - Weighted average pooling
    - Based on the distance from the central pixel
- Max pooling tends to work better than other pooling functions and convolutional strides

Pooling Functions



Pooling and Invariance

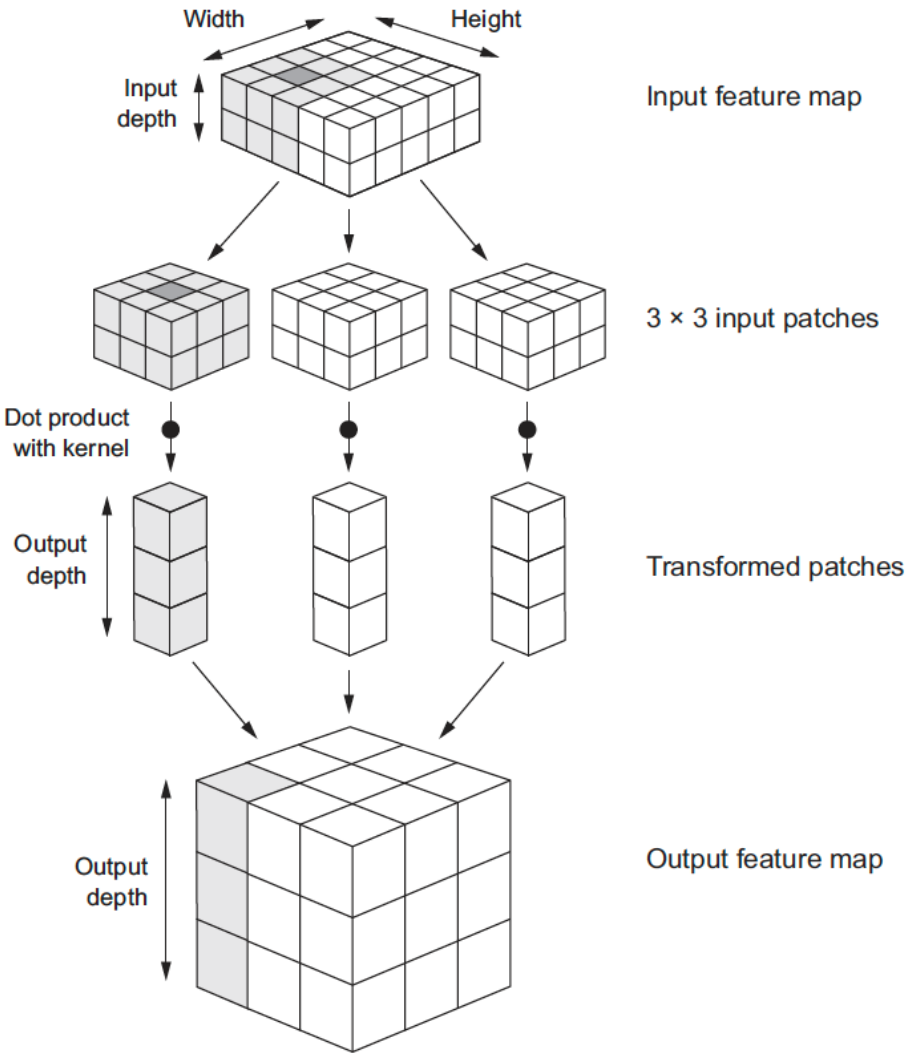
- A pooling unit that pools over multiple features that are learned with separate parameters can learn to be invariant to transformations of the input
- Here, a set of 3 learned filters and a max pooling unit can learn to become invariant to rotation



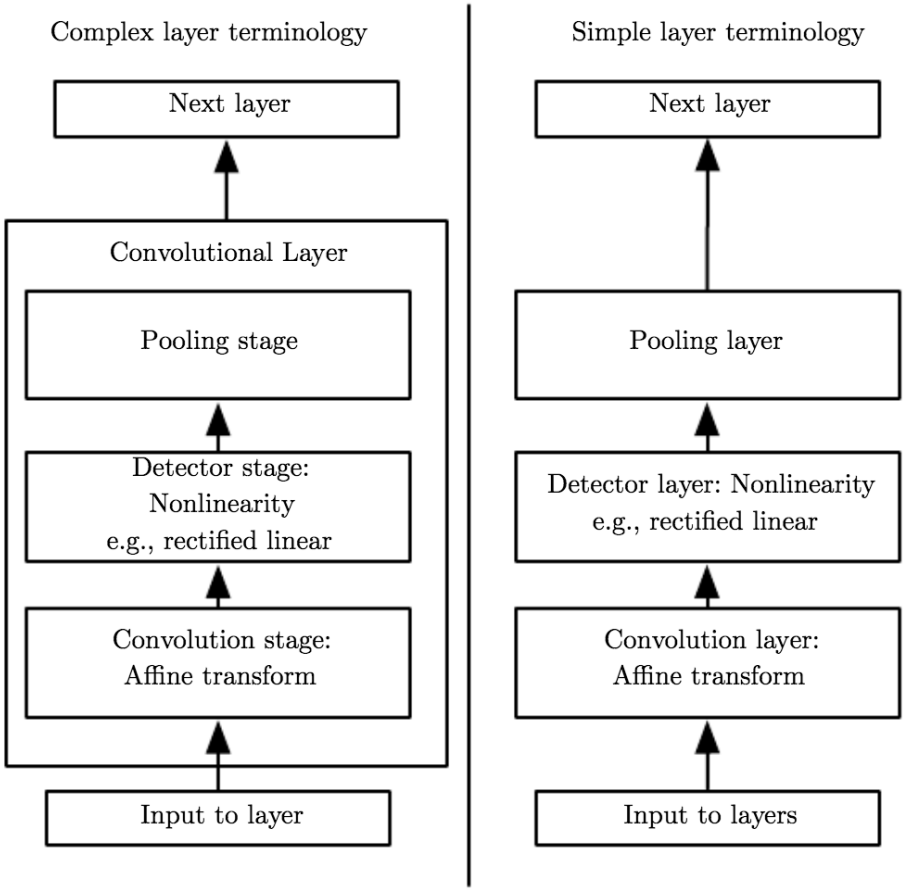
Terminology

- Convolutions operate over 3D tensors with two spatial axes, **height** and **width**, as well as a **depth** axis (or **channels** axis)
- For a color (RGB) image, the depth is equal to 3
- For black and white (greyscale) images, the depth is equal to 1
- The convolution operation extracts different **patches** from the input image and applies the same transformation to to each of them, resulting in a response map that is also a 3D tensor
- The response map has a width, height, and depth, all of which depend on the input image, filter, padding and stride
- Convolutions are defined by 2 key parameters:
  - Size of the filter
  - Depth of the output response map, i.e., how many filters are applied to the input
- Convolution works by sliding the filter over the 3D input image, stopping at every possible location, and extracting the 3D patch at each location
- Each 3D patch is transformed into a 1D vector
- All 1D vectors are then reassembled into a 3D output map

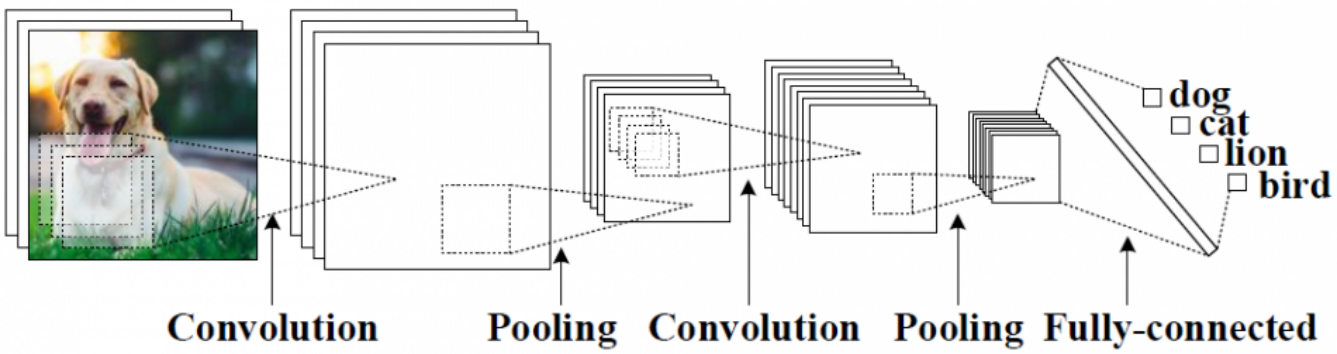
Convolution Schematic



Layer Terminology



CNN Schematic



Revisiting the MNIST Example

- Data loading and preparation don't change

```
import keras
from keras import layers
from keras import models
from keras.datasets import mnist
from keras.utils import to_categorical

(train_images, train_labels), (test_images, test_labels) = mnist.load_data()

train_images = train_images.reshape((60000, 28, 28, 1))
train_images = train_images.astype('float32') / 255

test_images = test_images.reshape((10000, 28, 28, 1))
test_images = test_images.astype('float32') / 255

train_labels = to_categorical(train_labels)
test_labels = to_categorical(test_labels)
```

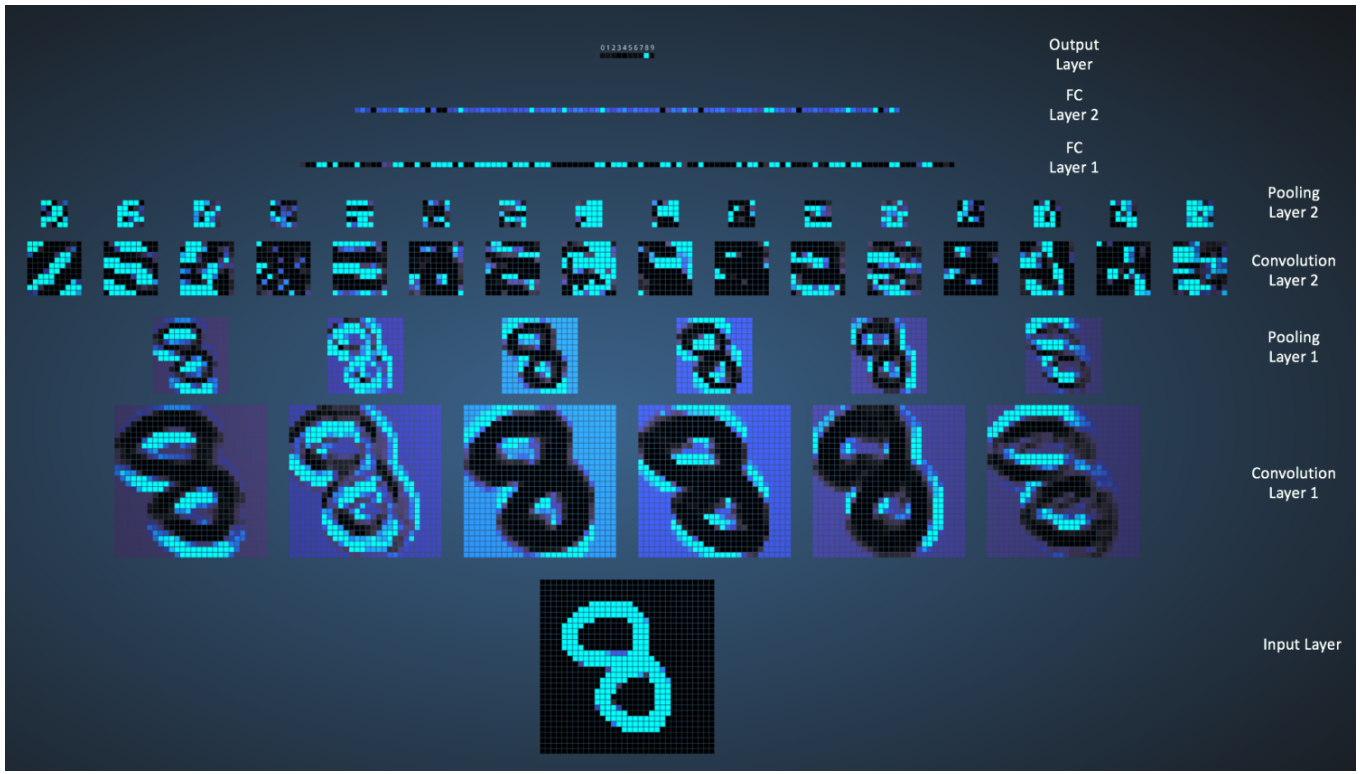
Revisiting the MNIST Example

```
# Still want a sequential, stack of layers
model = models.Sequential()
# Convolutional layer with 32 filters that are 3x3, relu activation function
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape=(28, 28, 1)))
# Pooling layer with 2x2 windows
model.add(layers.MaxPooling2D((2, 2)))
# Convolutional layer with 64 filters that are 3x3, relu activation function
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
# Pooling layer with 2x2 windows
model.add(layers.MaxPooling2D((2, 2)))
# Convolutional layer with 64 filters that are 3x3, relu activation function
model.add(layers.Conv2D(64, (3, 3), activation='relu'))

# Collapse the 3D tensor
model.add(layers.Flatten())
# Fully connected layer with 64 hidden units, relu activation function
model.add(layers.Dense(64, activation='relu'))
# Softmax output function with 10 classes
model.add(layers.Dense(10, activation='softmax'))

# Same optimizer, loss function and performance measure as before
model.compile(optimizer='rmsprop',
              loss='categorical_crossentropy',
              metrics=['accuracy'])
model.fit(train_images, train_labels, epochs=5, batch_size=64)
```

Revisiting the MNIST Example

```
>>> model.summary()
Layer (type)                 Output Shape              Param #
=================================================================
conv2d_1 (Conv2D)            (None, 26, 26, 32)        320
_________________________________________________________________
maxpooling2d_1 (MaxPooling2D)  (None, 13, 13, 32)      0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 11, 11, 64)        18496
_________________________________________________________________
maxpooling2d_2 (MaxPooling2D)  (None, 5, 5, 64)        0
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 3, 3, 64)          36928
_________________________________________________________________
flatten_1 (Flatten)          (None, 576)               0
_________________________________________________________________
dense_1 (Dense)              (None, 64)                36928
_________________________________________________________________
dense_2 (Dense)              (None, 10)                650
=================================================================
Total params: 93,322
Trainable params: 93,322
Non-trainable params: 0


>>> test_loss, test_acc = model.evaluate(test_images, test_labels)
>>> test_acc
0.99080000000000001
```

Revisiting the MNIST Example



Small Dataset CNN

- Go to the Jupyter notebook 5.2 on the course GitHub

Data Augmentation

- As we have seen, overfitting is caused by having too few training examples to learn from
- Data augmentation generates more training data from existing training examples by **augmenting** the samples via a number of random transformations
- These transformations should yield believable images
- Types of augmentation:
  - Rotation
  - Width or height shift
  - Shear
  - Zoom
  - Horizontal flip
  - Fill
- If you train a network using data-augmentation, it will never see the same input twice, but the inputs will still be heavily correlated - you're remixing known information, not producing new information
- May not completely escape overfitting due to this correlation
- Adding dropout can also help

Data Augmentation