Big Data and Security

Jeffrey Borowitz, PhD

Lecturer

Sam Nunn School of International Affairs

What are Neural Nets?

Neural Networks and “Deep Learning” (and AI?)

- In the last 10 years, neural nets have been responsible for tons of progress on a lot of AI type tasks
- Three questions:
  - How do we really know deep learning is “better”? Is it just hype?
  - How do they fit into our modelling taxonomy?
  - What makes them work so well?

Neural Networks

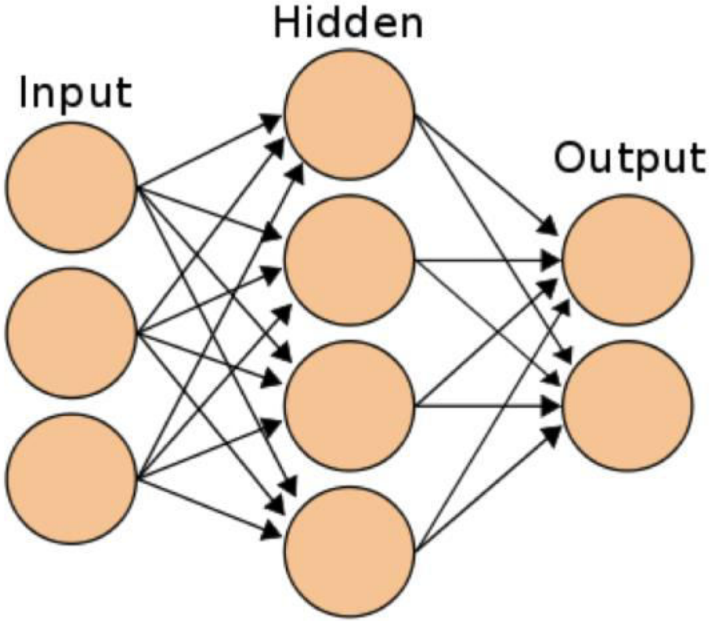
- A neural network is just a parametric model designed to capture strong nonlinearities.
- It is modelled on the interaction of neurons in brains
  - On the left hand side are data inputs
  - These each feed into a hidden layer of intermediate outputs
    - Depending how much flexibility you want, you could have multiple layers, and many neurons per layer
  - At each neuron, you might have something like a logistic model

$$out_i = \frac{1}{1 + \exp(\alpha + \beta x_1 + \gamma x_2 + \varepsilon_i}$$

  - At the next stage, you have logits based on these outputs:

$$final = \frac{1}{1 + \exp(a + b \cdot out_1 + c \cdot out_2 + e)}$$

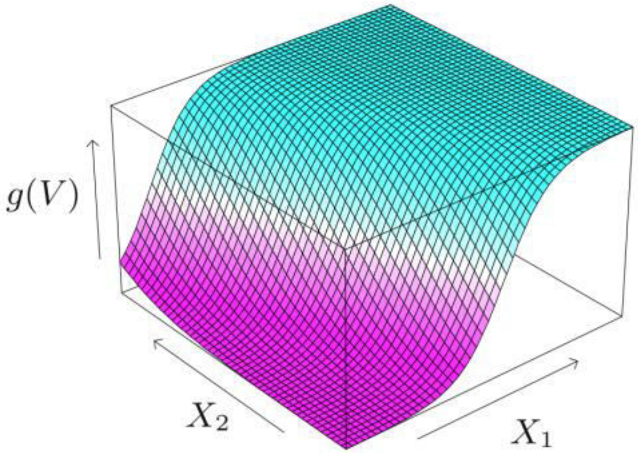
Neural Networks



Blog, G. (2016, October 7). The Evolution and Core Concepts of Deep Learning & Neural Netw orks. Retrieved from https://w ww.analyticsvidhy a.com/blog/2016/08/evolution-core-concepts-deep-learning-neural-netw orks/

Neural Networks

- They allow nonlinear functions of which can spike up in different combinations of directions

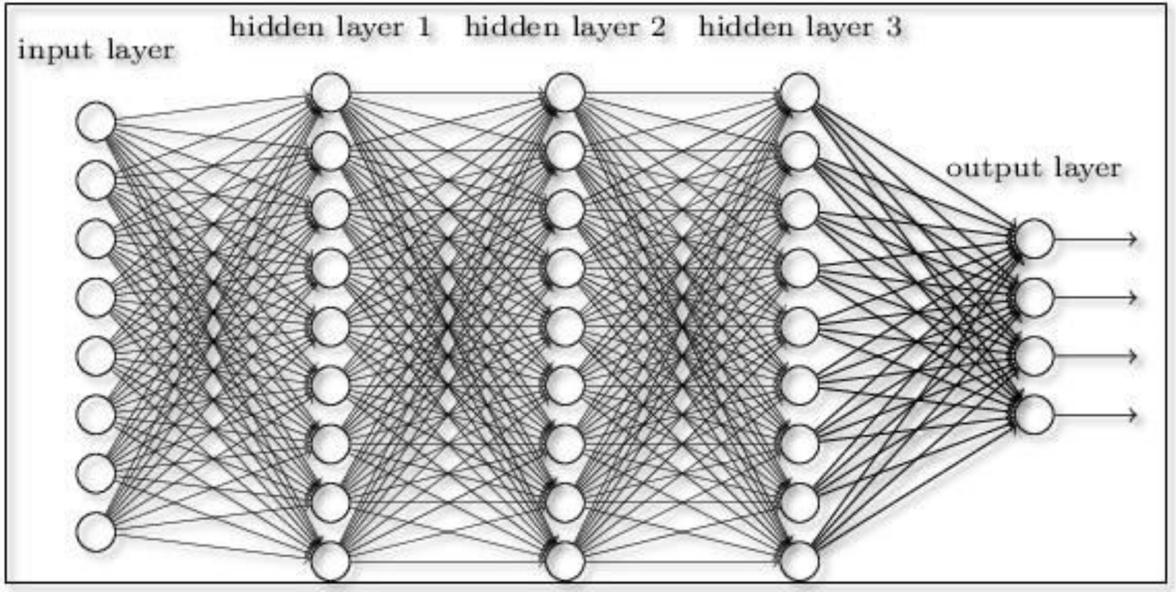


(n.d.). Retrieved from https://academicjournals.org/journal/AJB/article-full-text/CB147EB48416, figure 2

Neural Network Architectures

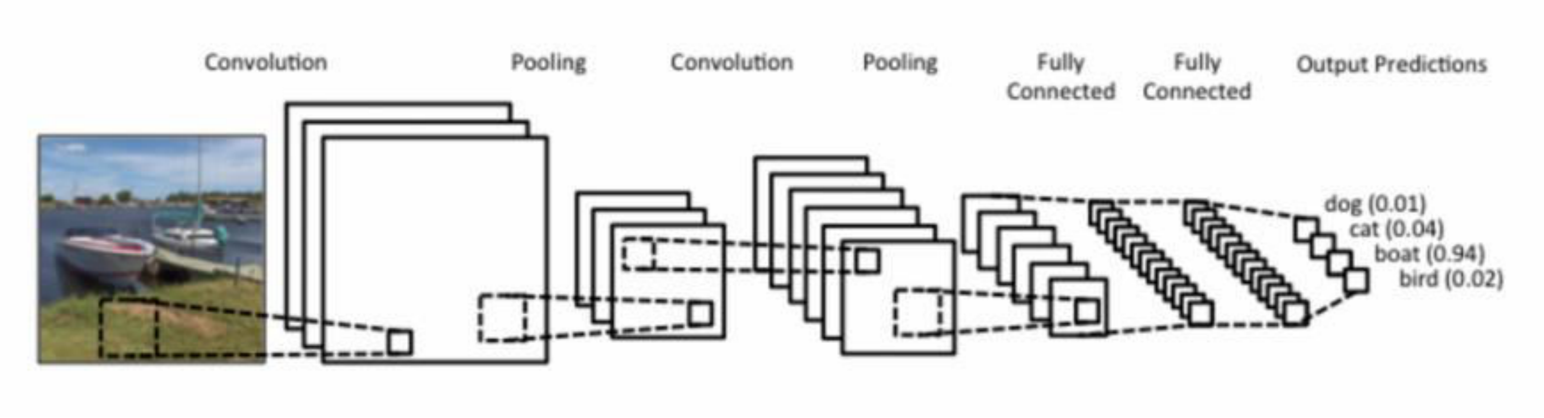
While neurons can be logistic functions, they can be other things too and there’s a lot of art in how people add/compose neural nets together.

Deep Neural Nets



Deep Neural Netw orks. (n.d.). Retrieved fromhttps://w ww.kdnuggets.com/2020/02/deep-neural-networks.html

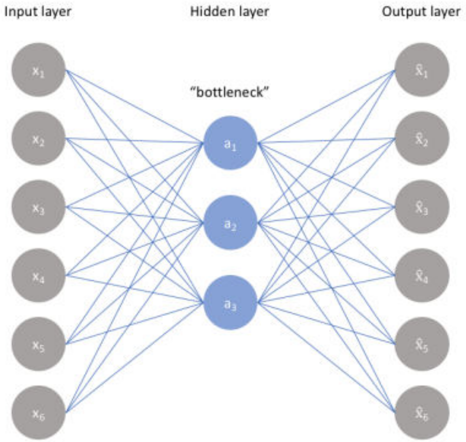
Convolutional Neural Nets



Sudhakar, S. (2017, August 2). Convolution Neural Netw ork. Retrieved from https://tow ardsdatascience.com/convolution-neural-netw ork-e9b864ac1e6c

Auto-Encoders

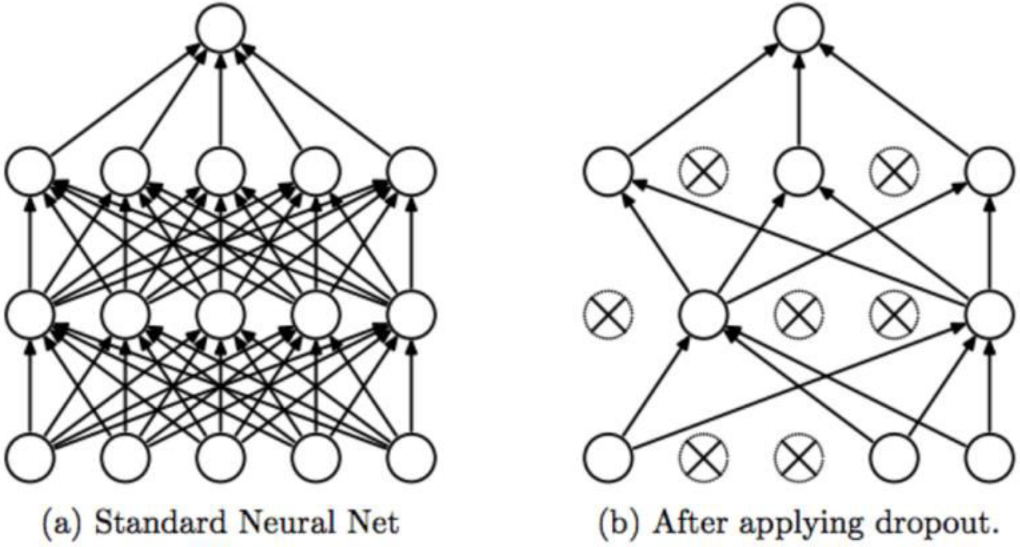
- There is a lot of text data (books, webpages, emails)
- But not a lot of it is framed as independent and dependent variables
- Autoencoders



Salam, I. (2019, August 20). Autoencoders - Guide and Code in TensorFlow 2.0. Retrieved from https://medium.com/red-buffer/autoencoders-guide-and-code-in-tensorflow-2-0-a4101571ce56

Dropout

- Avoid overfitting by randomly removing some nodes



Chm. (2019, January 10). Neural Netw ork and Dropouts. Retrieved from https://mc.ai/neural-netw ork-and-dropouts/

Neural Networks: Pros and Cons

Pro:

- Neural networks can fit very nonlinear functions
- They can benefit from more data for longer than other models

Con:

- They have many degrees of freedom
- It’s hard to get a neural network to converge, because there are “too many wiggles”
- Overfitting can be a problem

Neural Network: Practical Characteristics

First, people are still learning. It often helps to build “deep” networks

- This means more layers between the start and the prediction

For images, a “convolutional” pattern works really well:

- Data from a group of nearby pixels goes into a single neuron
- Then that neuron’s output goes to most of the places in the next level

For text, a “recurrent” pattern works well, where the output of one group feeds back to itself.

- Also, an “attention” based pattern where the previous text that matters can be selected

Lesson Summary

- A neural network is a parametric model designed to capture strong nonlinearities.
- While neurons can be logistic functions, there’s a lot of art in how people add/compose neural nets together
  - Ex. Deep neural nets, convolutional neural nets
- Dropout is how you part of how you overfitting by randomly removing some nodes