Deep Learning New Frontiers

Power of Neural Nets

- Universal Approximation Theory
  - A feed-forward network with a single layer is sufficient to approximate, to an arbitrary precision, any continuous function
  - Caveat
    - Number of hidden units could be large
    - The resulting model may not generalize

AI "Hype"

- Caused false hope for computer scientists and public

Limitations

- "Understanding Neural Networks Requires Rethinking Generalization"
- As you introduce randomness, test data will yield more random results, but training data will yield almost 100% accuracy
- Neural Networks are excellent function approximators
  - IF they have training data

Neural Network Attribute Models

- From data used to train model we need accurate data to yield proper results
- Example: Cars in autopilot crash due to new pylons not in Google Street View
- Perturbations can fool neural networks into mis-classifying data
  - Called Adversarial Attack on Neural Networks

Adversarial attacks on Neural Networks

- Adversarial Image
  - Modify image to increase error
  - $x \leftarrow x + \eta \frac{\partial J(w, x, y)}{\partial x}$
  - "How does a small change in the input increase our loss"

Algorithmic Bias

- Racial, age, gender bias and more

Limitations

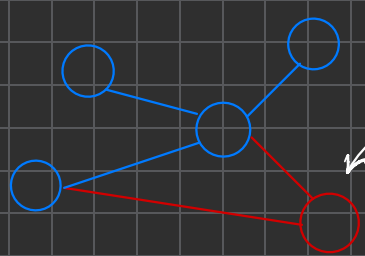
- Many limitations
- Difficult to encode structure and prior knowledge during learning
- Struggles to extrapolate

Encoding structure into deep learning

- CNNs
  - Use spatial structure through convolution
- Graphs as a structure for representing data
  - State machines
  - Social Networks
  - Mobility and transport

Graph Convolutional Networks

- Review: Sliding kernel "filters"
- Same idea applies for graph convolutional networks



Kernel pays attention to node and local connectivity

Applications of Graph Neural Networks

- Molecular Discovery
  - Halicin: novel antibiotic discovered via deep learning
- Traffic prediction
  - ETA improvements with Google Maps
- Covid-19 Forecasting
  - Spatio-temporal data

Learning From 3D Data

- Point clouds are unordered sets with spatial dependence between points
- Extending Graph CNNs to Pointclouds
  - Capture local geometric features of point clouds while maintaining order invariance

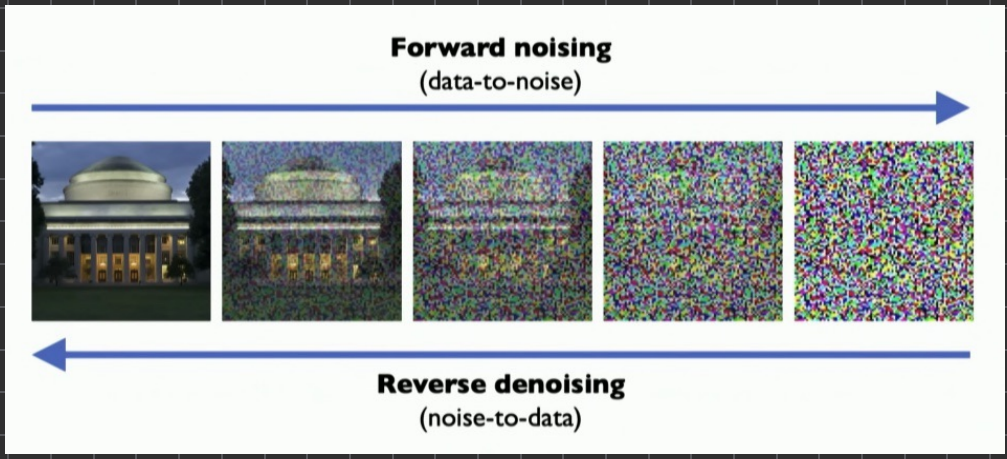
Generative AI and Diffusion Models

- In Lecture 4, we talked about VAEs and GANs
  - Limitations
    - Mode Collapse
    - Generate OOD
    - Hard to train
  - Challenges
    - Stability
    - Efficiency
    - Quality
    - Novelty
- Diffusion Models and Text-to-Image models tackle these challenges

Diffusion Models

- VAEs and GANs
  - Generating samples in one shot directly from low-dimensional latent variables
- Diffusion
  - Generate samples iteratively by repeatedly removing noise

The Diffusion Process



Forward Noising

Steps

1.) Given an image, randomly sample a random noise pattern

2.) Progressively add more noise to the image

Reverse Denoising

Goal: Given image at T, can we learn to estimate image at T-1?

- Look at pixel-wise difference between each step

Sampling Brand New Generations

- Going from a completely random noise state, iteratively work towards noise free image
- Diffusion models generate new, diverse ideas

Generating images from Natural Language

- Embedding used to translate text to images

Beyond images: Molecular Design

- Generating molecules in 3D
- Generating novel proteins