- Limitations:
- Adversarial attack:
- GCN: extract features from graph.
- 3D Data: point clound
- Automated Machine Learning(Auto ML)
- Auto AI: end-to-end.

Limitations:

1. data hungry

2. computationally intensive to train

3. easily fooled byu adversarial examples.

4. poor at representing uncertainty.

5. uninterpretability, diffuct to trust

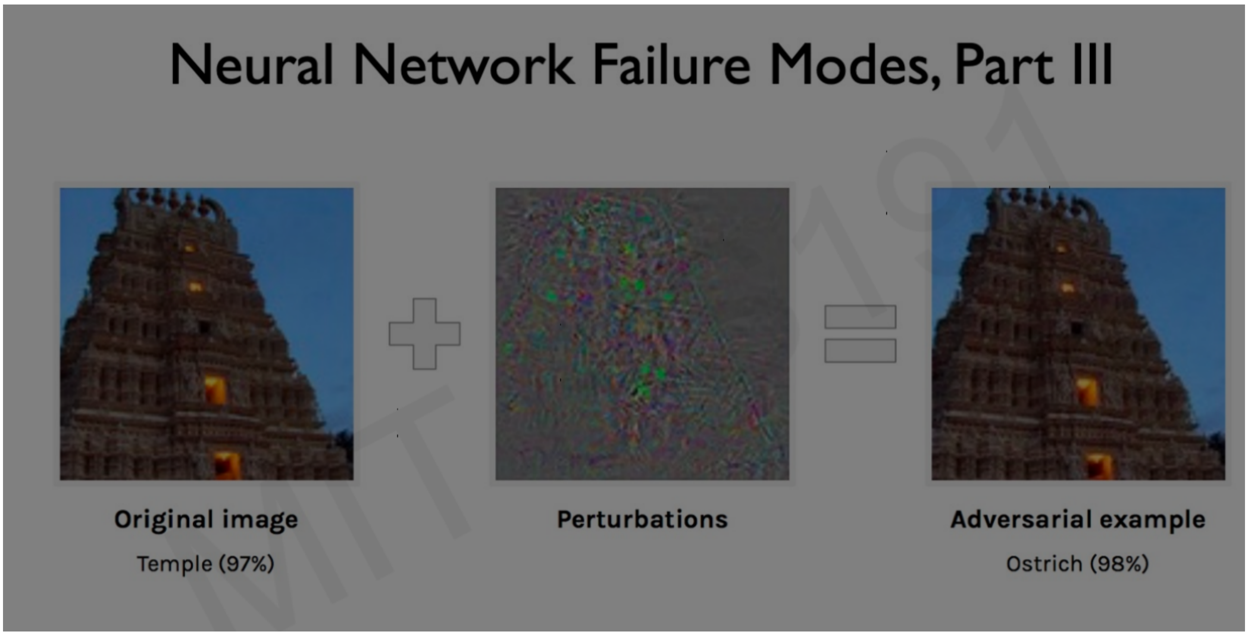
6.diffcult to encode structure.

7. require prior knowledge. induce bias.

8.finicky to optimize.

9.require expert knowledge to design and fine tune architecture.

adversarial attack:



Neural Network Failure Modes, Part III

Original image

Temple (97%)

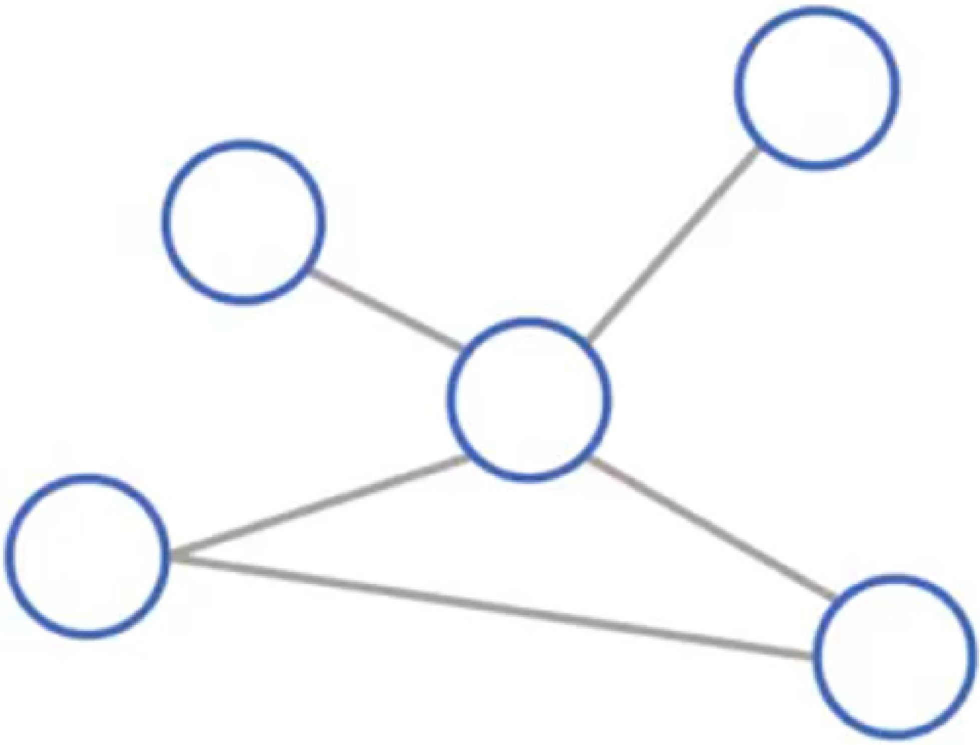
Perturbations

Adversarial example

Ostrich (98%)

GCN:

Graph Convolutional Networks



edges define the relationships between nodes.

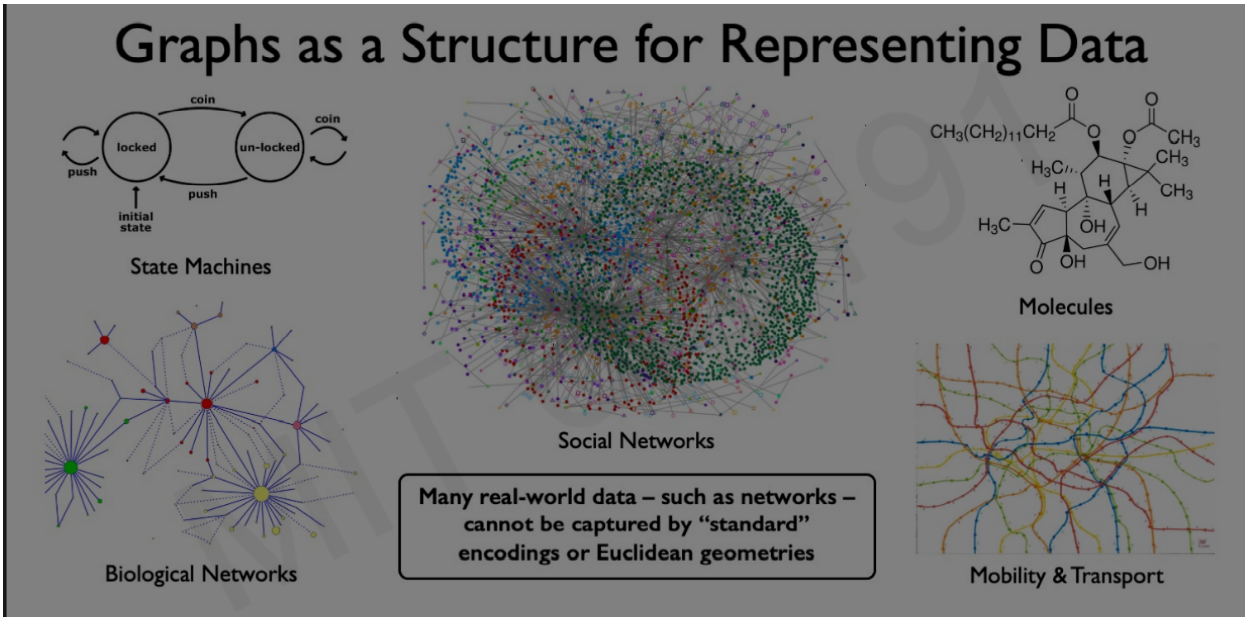
How we extract information from graph?

take a kernel (weight matrix)

kernel travel around, pop around to different node.

pick up features of local connectivity from neighborhood.

Application:



Graphs as a Structure for Representing Data

State Machines

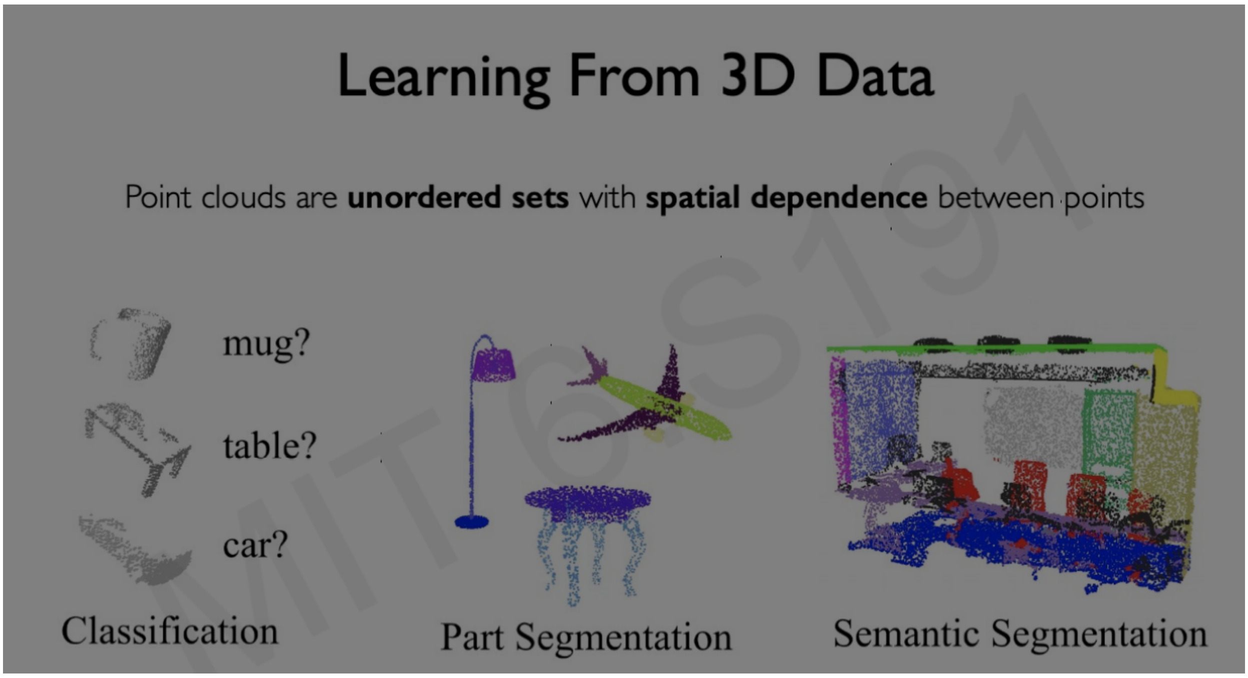
Social Networks

Molecules

Biological Networks

Many real-world data – such as networks – cannot be captured by "standard" encodings or Euclidean geometries

Mobility & Transport



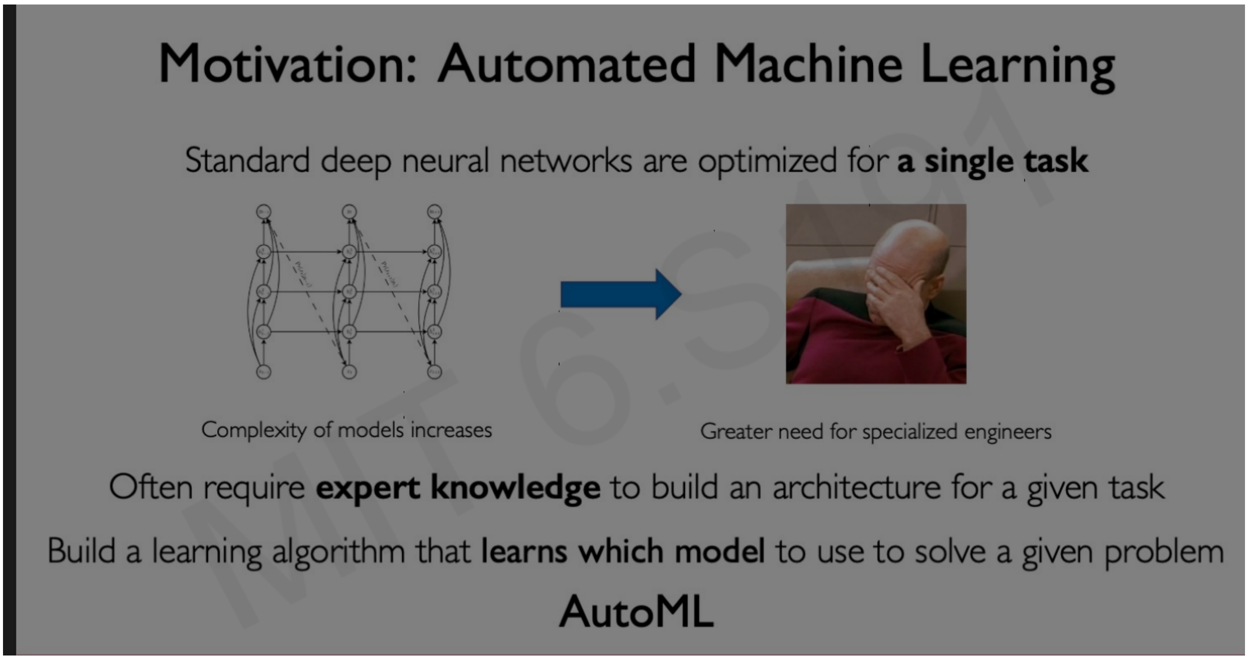
Learning From 3D Data

Point clouds are **unordered sets** with **spatial dependence** between points

Classification

Part Segmentation

Semantic Segmentation



Motivation: Automated Machine Learning

Standard deep neural networks are optimized for **a single task**

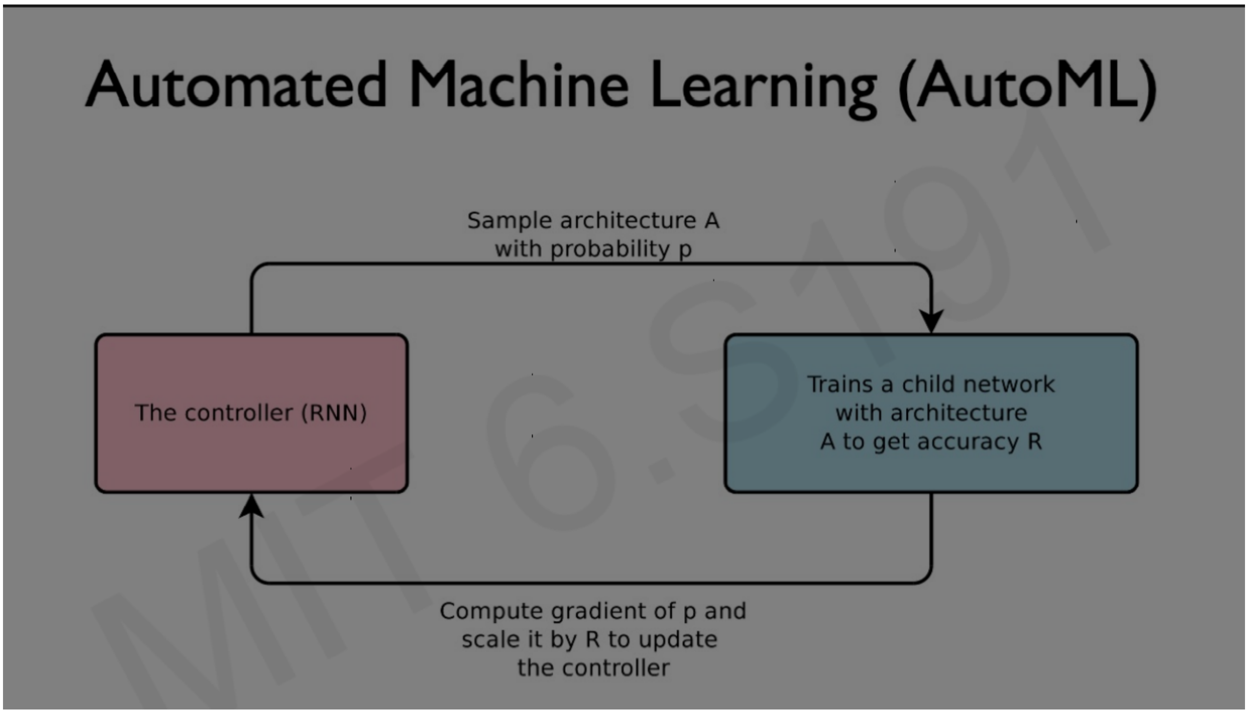
Complexity of models increases

Greater need for specialized engineers

Often require **expert knowledge** to build an architecture for a given task

Build a learning algorithm that **learns which model** to use to solve a given problem

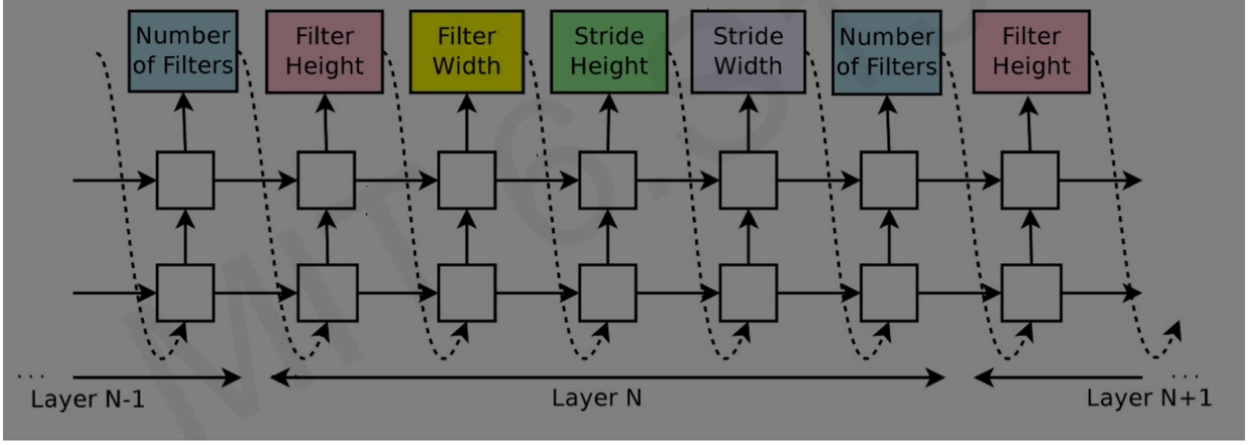
AutoML



Automated Machine Learning (AutoML)

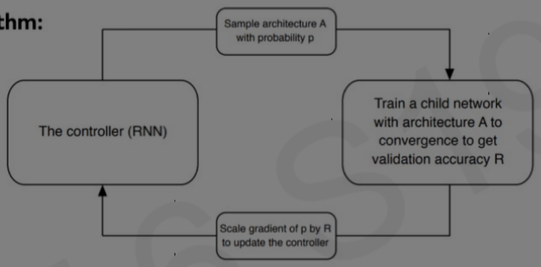
AutoML: Model Controller

At each step, the model samples a brand new network



Learning Architectures for Image Recognition

Neural architecture search algorithm:



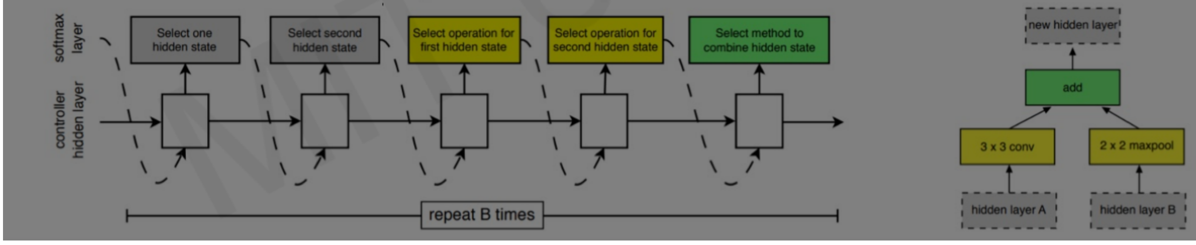
Sample architecture A with probability p

The controller (RNN)

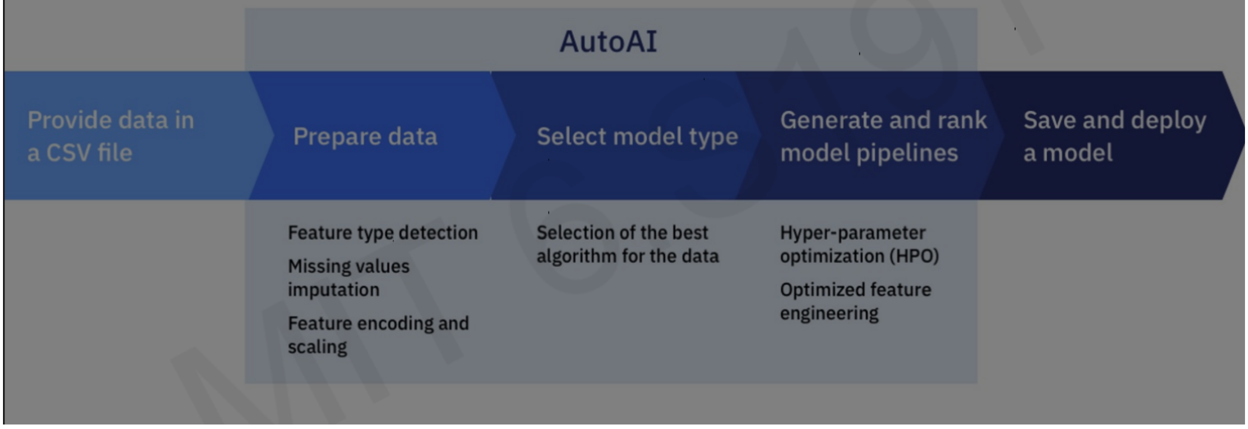
Train a child network with architecture A to convergence to get validation accuracy R

Scale gradient of p by R to update the controller

Controller architecture for constructing convolutional layers:



From AutoML to AutoAI



AutoAI

Provide data in a CSV file

Prepare data

Select model type

Generate and rank model pipelines

Save and deploy a model

Feature type detection

Missing values imputation

Feature encoding and scaling

Selection of the best algorithm for the data

Hyper-parameter optimization (HPO)

Optimized feature engineering