

Deep Learning Limitations and New Frontiers

Final Class Project

Option 1:

Choose one of the topic dealt with in the course, study deeply the state of the art, compare solutions in the literature, possibly executing comparative tests

Option 2:

Present a novel deep learning research idea or application ideally concerning your research field

The Rise of Deep Learning

'Deep Voice' Software Can Clone Anyone's Voice With Just 3.7 Seconds of Audio

Using snippets of voices, Baidu's 'Deep Voice' can generate new speech, accents, and tones.

Let There Be Sight: How Deep Learning Is Helping the Blind 'See'



Technology outpacing security measures

AI beats docs in cancer spotting

A new study provides a fresh example of machine learning as an important diagnostic tool. Paul Hsieh reports.

AI Can Help In Predicting Cryptocurrency Value



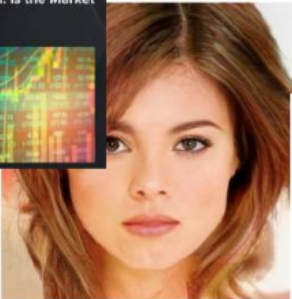
'Creative' AlphaZero leads way for chess computers and, maybe, science

Former chess world champion Garry Kasparov likes what he sees of computer that could be used to find cures for diseases

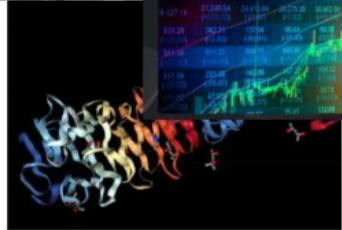


How an A.I. 'Cat-and-Mouse Game' Generates Believable Fake Photos

By Gabe HELL and KEITH COLLINS JAN 3, 2019



Stock Predictions Based On AI: Is the Market Truly Predictable?



Google's DeepMind acs protein folding

By Robert F. Service | Dec. 6, 2018, 12:05 PM



Complex of bacteria-infecting viral proteins modeled in CASP 13. The complex contains proteins that were modeled individually. PROTEIN DATA BANK



DEEPMIND I STARCRAFT TRIUMPH



Neural networks everywhere

New chip reduces neural networks' power consumption by up to 95 percent, making them practical for battery-powered devices.

Deep L

Wed, 04/16/2019 - 8:00am | Comment | by Kenny Walker - Digital Reporter - @RandDMagazine



AI-generated faces show how far AI image generation has come in just four years

What's on the right aren't real; they're the product of machine learning



Automation And Algorithms: De-Risking Manufacturing With Artificial Intelligence

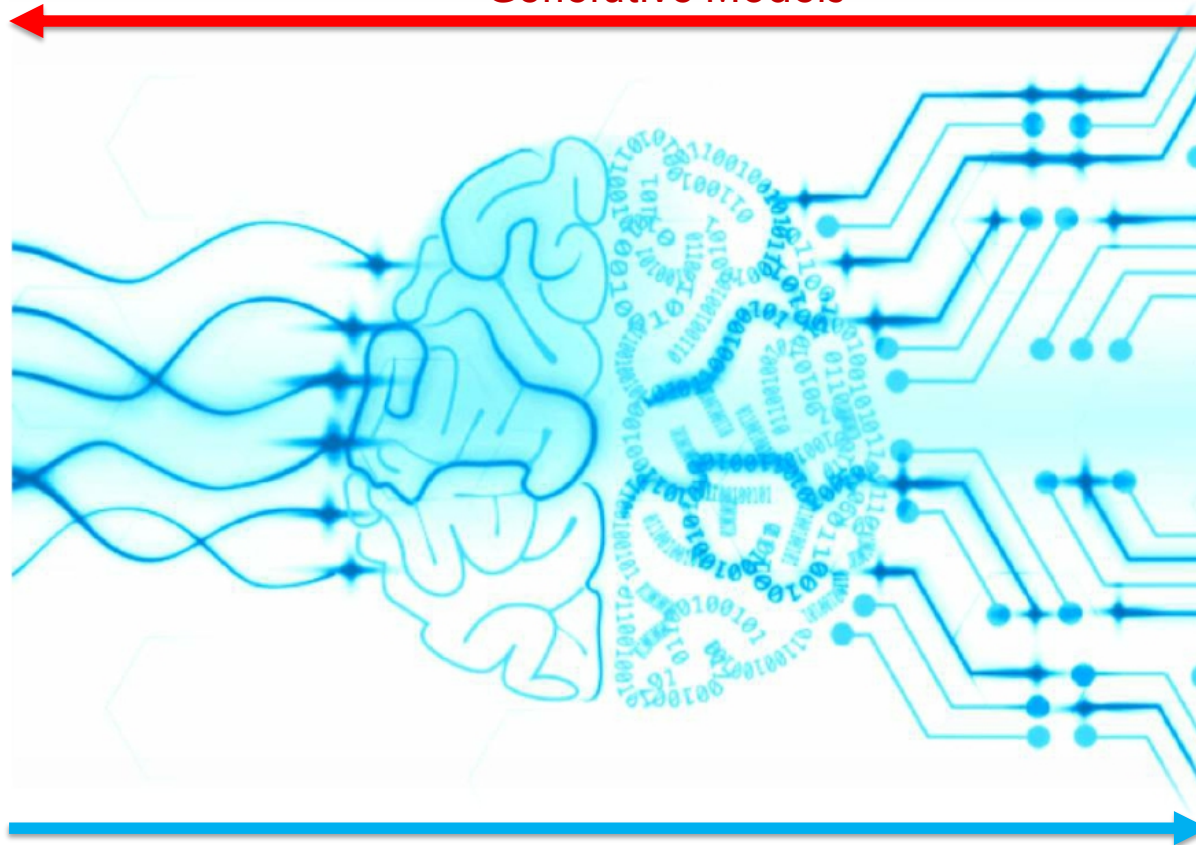
Sarah Goehrkke Contributor Manufacturing | Focus on the industrialization of additive manufacturing.

TWEET THIS

The two key applications of AI in manufacturing are pricing and manufacturability feedback

So far..

Generative Models



Data

- Signals
- Images
- Sensors
- ...

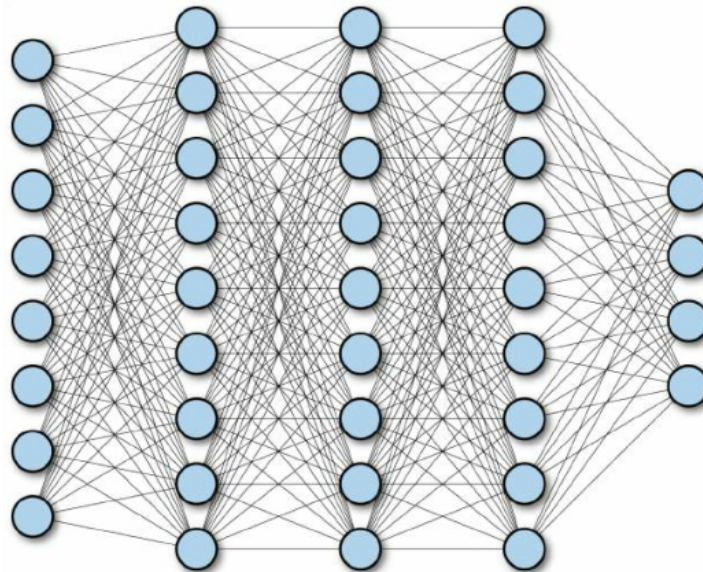
Decision

- Prediction
- Detection
- Action
- ...

Power of Neural Nets

Universal Approximation Theorem

A feedforward network with a single layer is sufficient to approximate, to an arbitrary precision, any continuous function.



Hornik et al. *Neural Networks*. (1989)

Power of Neural Nets

Universal Approximation Theorem

A feedforward network with a single layer is sufficient to approximate, to an arbitrary precision, any continuous function.

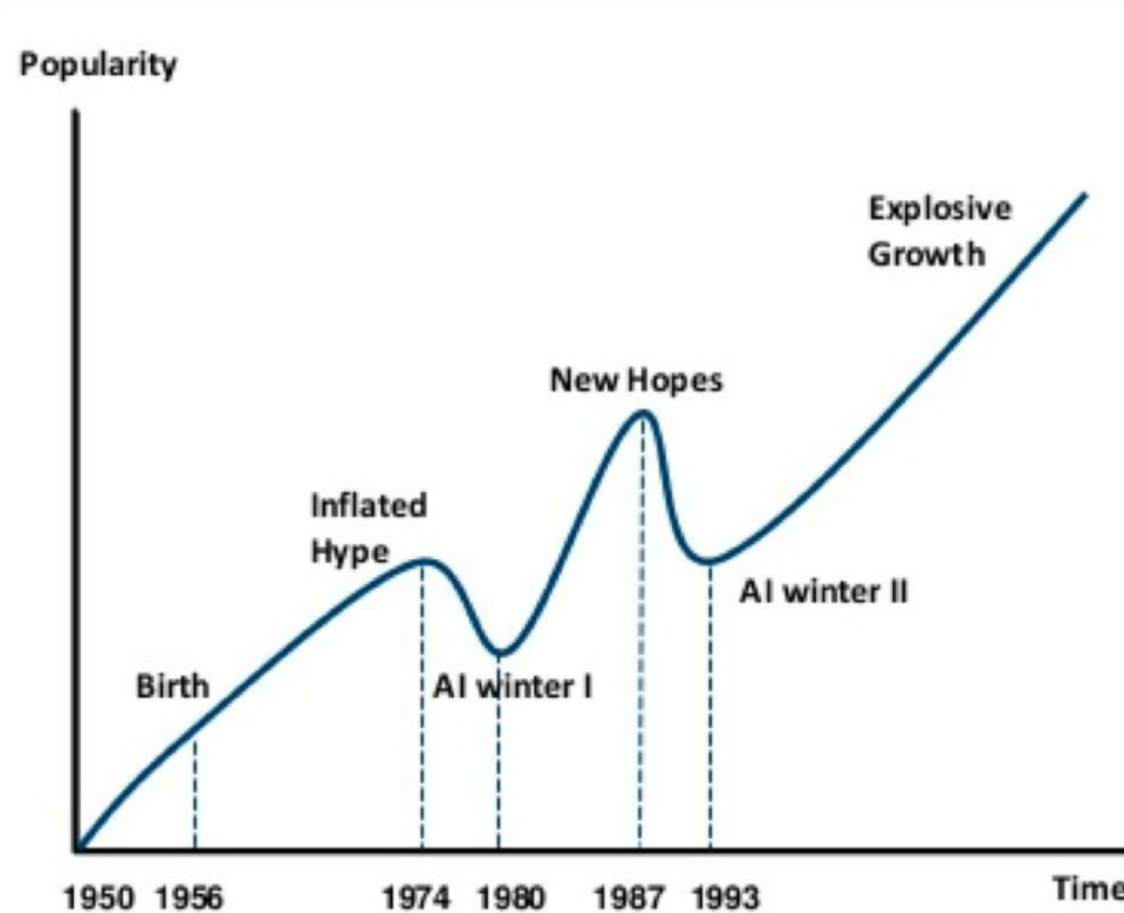
Caveats:

The number of hidden units may be infeasibly large

The resulting model may not generalize

Hornik et al. *Neural Networks*. (1989)

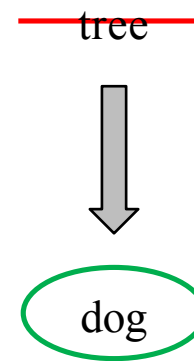
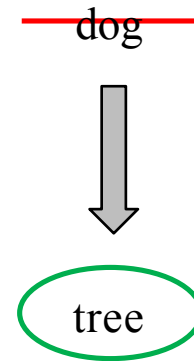
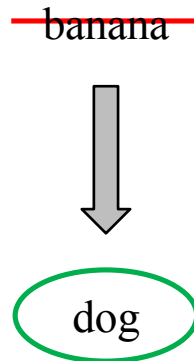
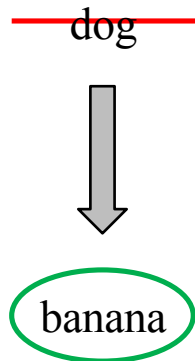
Artificial Intelligence "Hype": Historical Perspective



Limitations

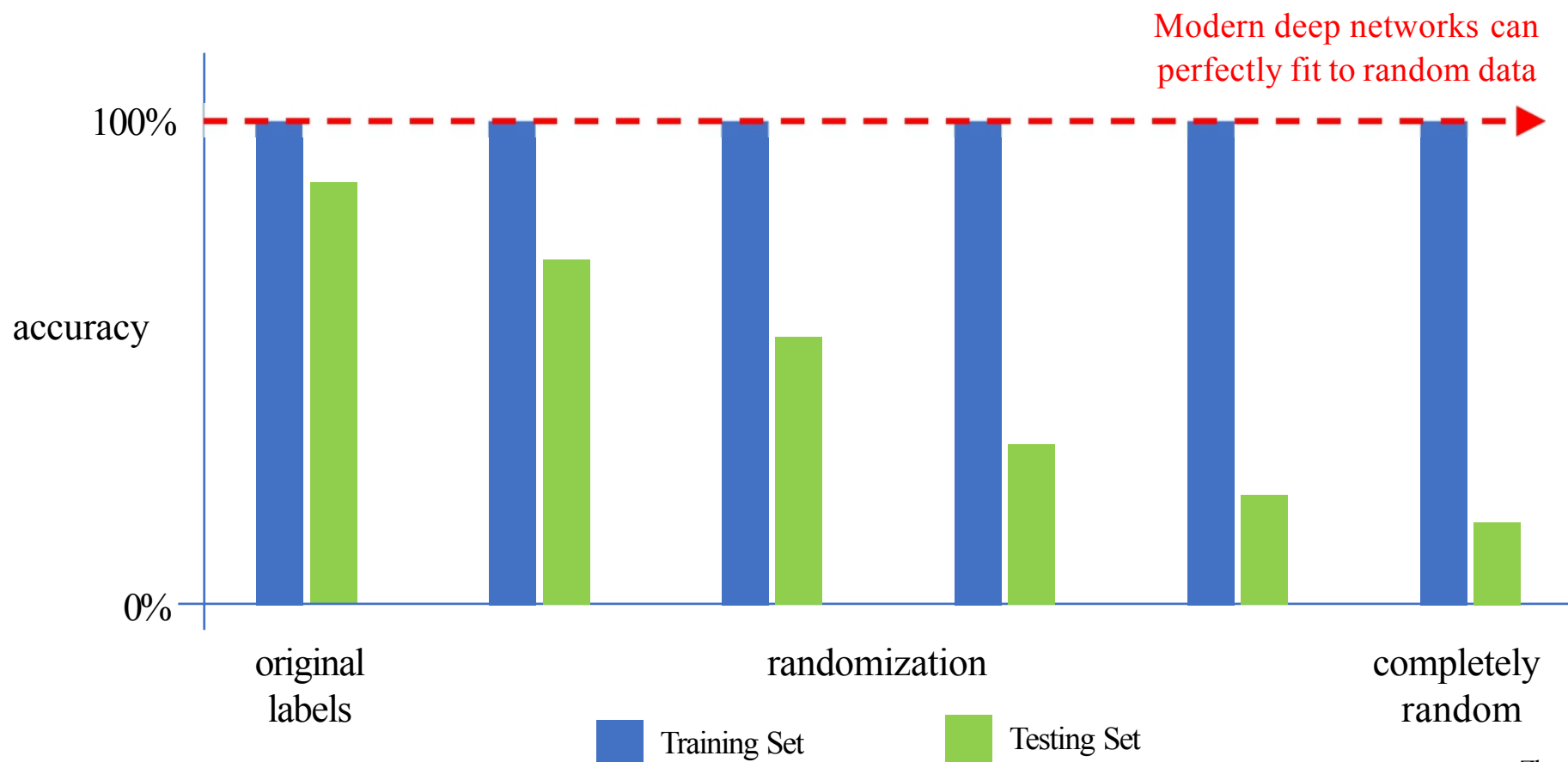
Rethinking Generalization

“Understanding Deep Neural Networks Requires Rethinking Generalization



Zhang et al. *ICLR*. (2017)

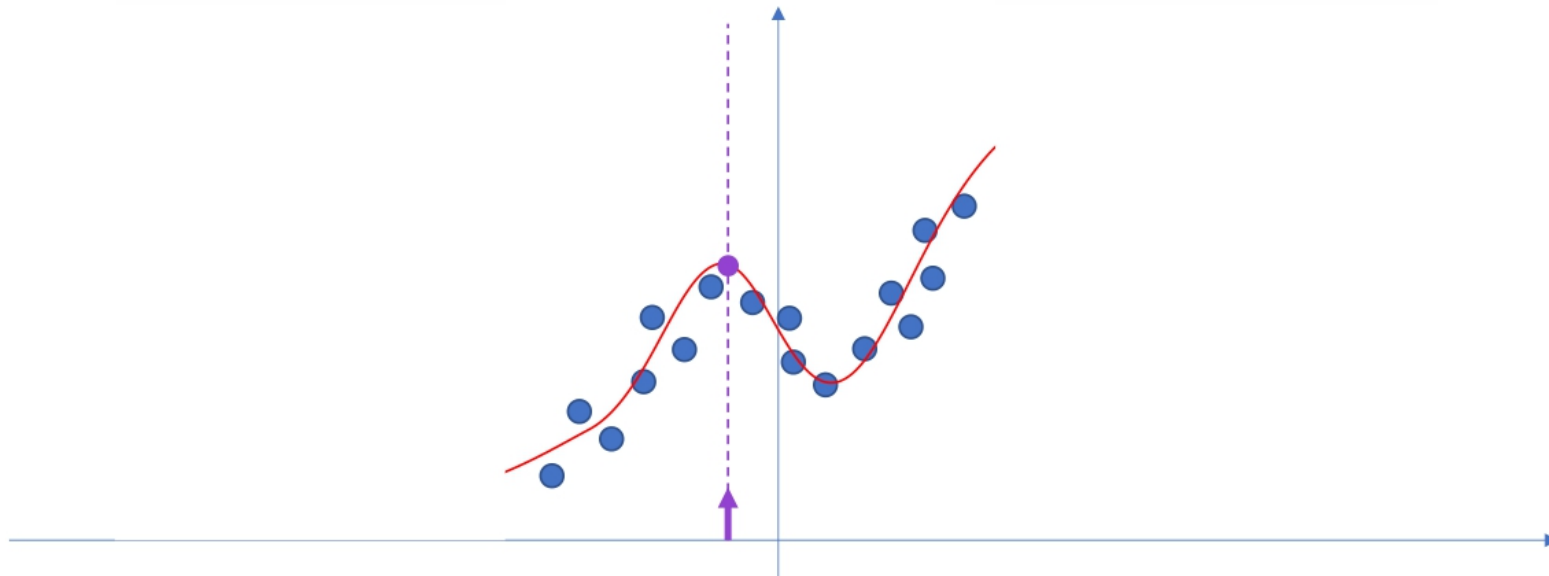
Capacity of Deep Neural Networks



Zhang et al. *ICLR*. (2017)

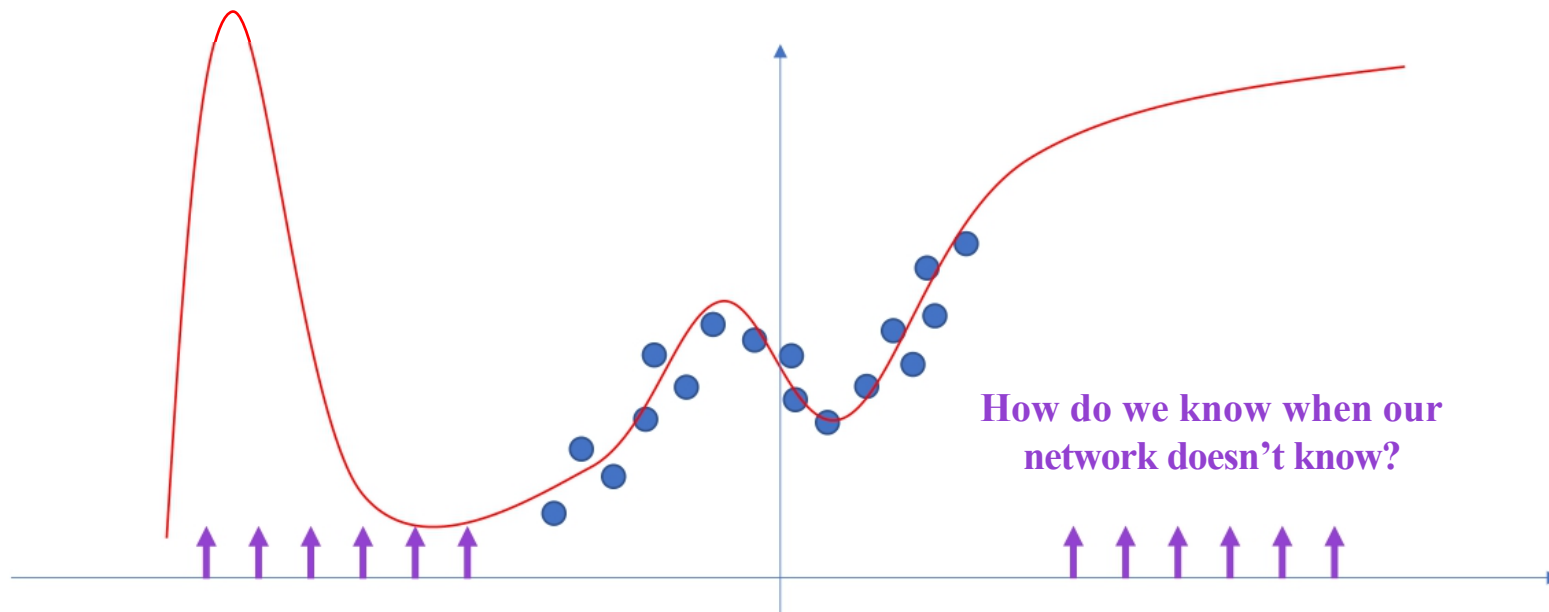
Neural Networks as Function Approximators

Neural networks are **excellent** function approximators



Neural Networks as Function Approximators

Neural networks are **excellent** function approximators
...when they have training data

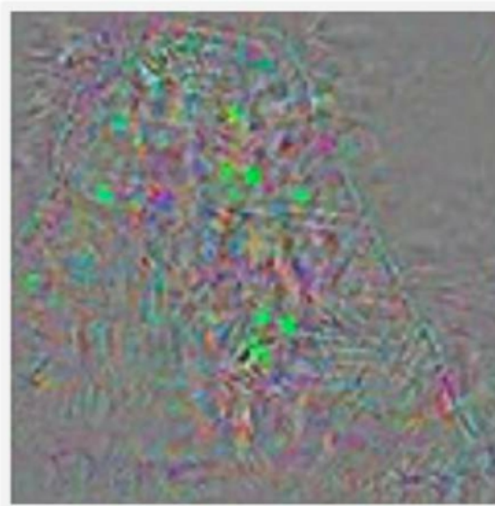


Adversarial Attacks on Neural Networks

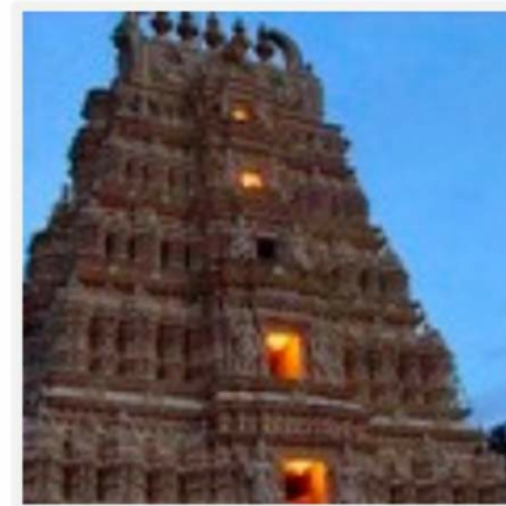


Original image

Temple (97%)



Perturbations



Adversarial example

Ostrich (98%)

Despois. “Adversarial examples and their implications” (2017).

Adversarial Attacks on Neural Networks

Remember:

We train our networks with gradient descent

$$\theta \leftarrow \theta - \eta \frac{\partial J(\theta, x, y)}{\partial \theta}$$

Fix your image x ,
and true label y

“How does a small change in weights decrease our loss”

Adversarial Attacks on Neural Networks

Adversarial Image:

Modify image to increase error

$$x \leftarrow x + \eta \frac{\partial J(\theta, x, y)}{\partial x}$$

Fix your weights θ ,
and true label y

“How does a small change in the input increase our loss”

Synthesizing Robust Adversarial Examples



■ classified as turtle ■ classified as rifle
■ classified as other

Athalye et al. *ICML*. (2018)

Neural Network Limitations...

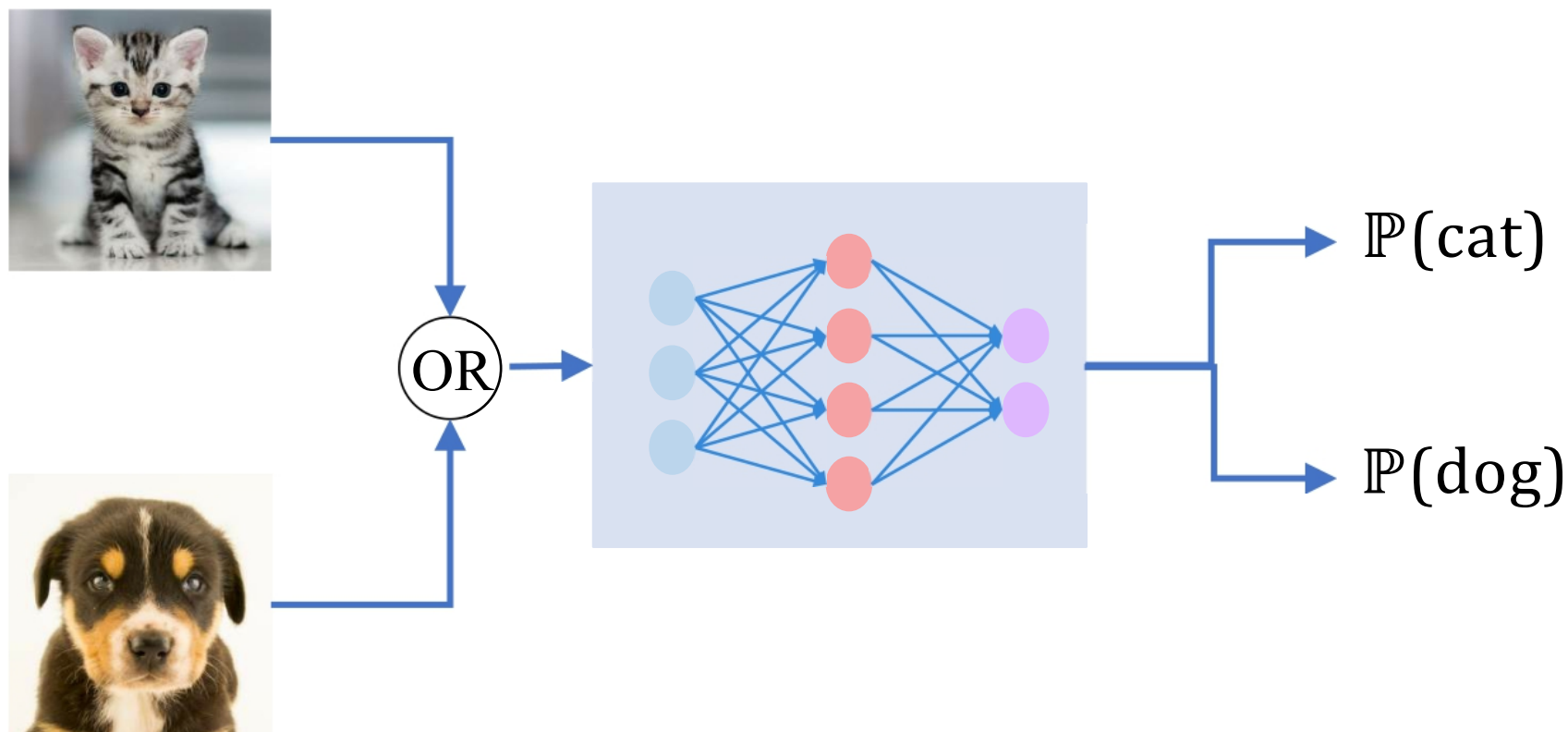
- Very **data hungry** (eg. often millions of examples)
- **Computationally intensive** to train and deploy (tractably requires GPUs)
- Easily fooled by **adversarial examples**
- Can be subject to **algorithmic bias**
- Poor at **representing uncertainty** (how do you know what the model knows?)
- Uninterpretable **black boxes**, difficult to trust
- **Finicky to optimize**: non-convex, choice of architecture, learning parameters
- Often require **expert knowledge** to design, fine tune architectures

Neural Network Limitations...

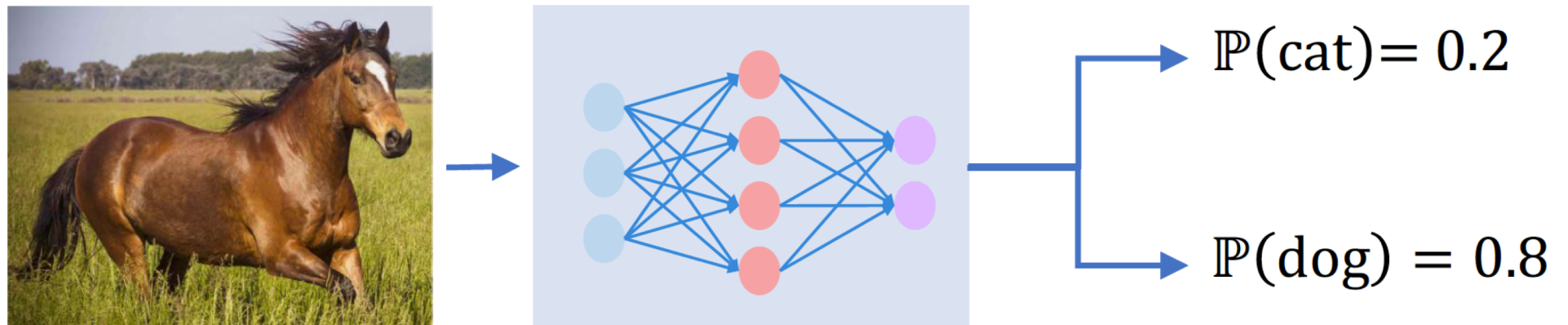
- Very **data hungry** (eg. often millions of examples)
- **Computationally intensive** to train and deploy (tractably requires GPUs)
- Easily fooled by **adversarial examples**
- Can be subject to **algorithmic bias**
- Poor at **representing uncertainty** (how do you know what the model knows?)
- Uninterpretable **black boxes**, difficult to trust
- **Finicky to optimize**: non-convex, choice of architecture, learning parameters
- Often require **expert knowledge** to design, fine tune architectures

New Frontiers 1: Bayesian Deep Learning

Why Care About Uncertainty?



Why Care About Uncertainty?



Remember: $\mathbb{P}(\text{cat}) + \mathbb{P}(\text{dog}) = 1$

Bayesian Deep Learning for Uncertainty

Network tries to learn output, \mathbf{Y} , directly from raw data, \mathbf{X}

Find mapping, f , parameterized by weights $\boldsymbol{\theta}$ such that
$$\min \mathcal{L}(\mathbf{Y}, f(\mathbf{X}; \boldsymbol{\theta}))$$

Bayesian neural networks aim to learn a posterior over weights,
$$\mathbb{P}(\boldsymbol{\theta} | \mathbf{X}, \mathbf{Y}):$$

$$\text{Intractable! } \mathbb{P}(\boldsymbol{\theta} | \mathbf{X}, \mathbf{Y}) = \frac{\mathbb{P}(\mathbf{Y} | \mathbf{X}, \boldsymbol{\theta}) \mathbb{P}(\boldsymbol{\theta})}{\mathbb{P}(\mathbf{Y} | \mathbf{X})}$$

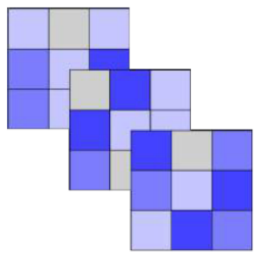
Elementwise Dropout for Uncertainty

Evaluate T stochastic forward passes through the network $\{\boldsymbol{\theta}_t\}_{t=1}^T$

Dropout as a form of stochastic sampling $z_{w,t} \sim \text{Bernoulli}(p) \quad \forall w \in \boldsymbol{\theta}$

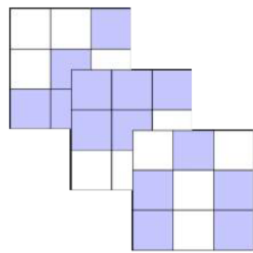
Unregularized Kernel

$\boldsymbol{\theta}$



Bernoulli Dropout

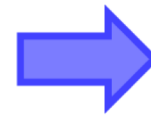
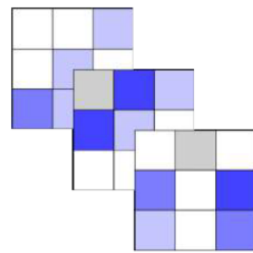
$z_{\boldsymbol{\theta},t}$



=

Stochastic Sampled

$\boldsymbol{\theta}_t$



$$\mathbb{E}(\hat{Y}|\mathbf{X}) = \frac{1}{T} \sum_{t=1}^T f(\mathbf{X}|\boldsymbol{\theta}_t)$$

$$\text{Var}(\hat{Y}|\mathbf{X}) = \frac{1}{T} \sum_{t=1}^T f(\mathbf{X})^2 - \mathbb{E}(\hat{Y}|\mathbf{X})^2$$

0 1 >1

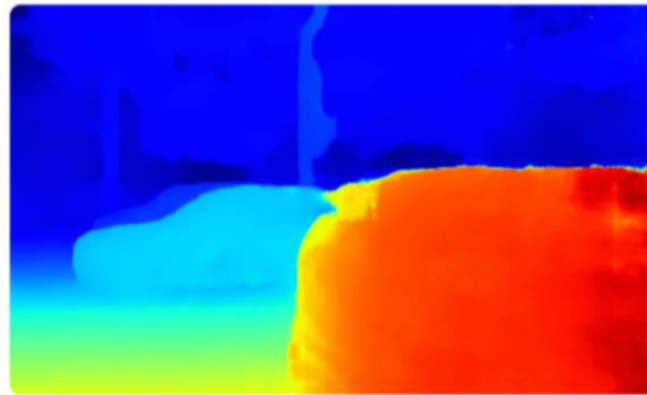
Gal and Ghahramani, *ICML*, 2016.

Amini, Soleimany, et al., *NIPS Workshop on Bayesian Deep Learning*, 2017.

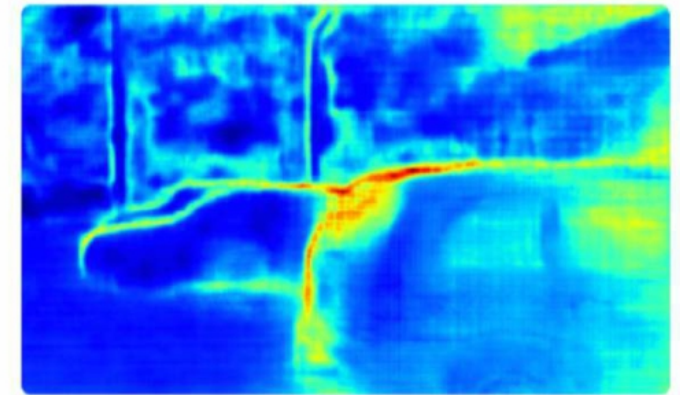
Model Uncertainty Application



Input image



Predicted Depth



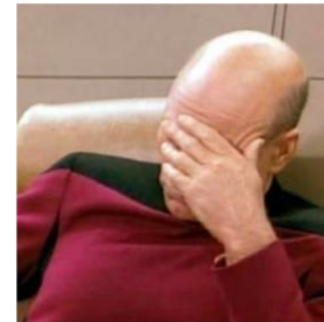
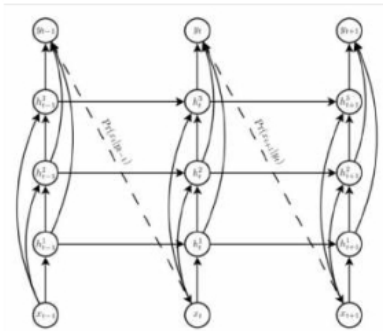
Model Uncertainty

Kendall, Gal, *NIPS*, 2017.

New Frontiers II: Learning to Learn

Motivation: Learning to Learn

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



Complexity of models increases

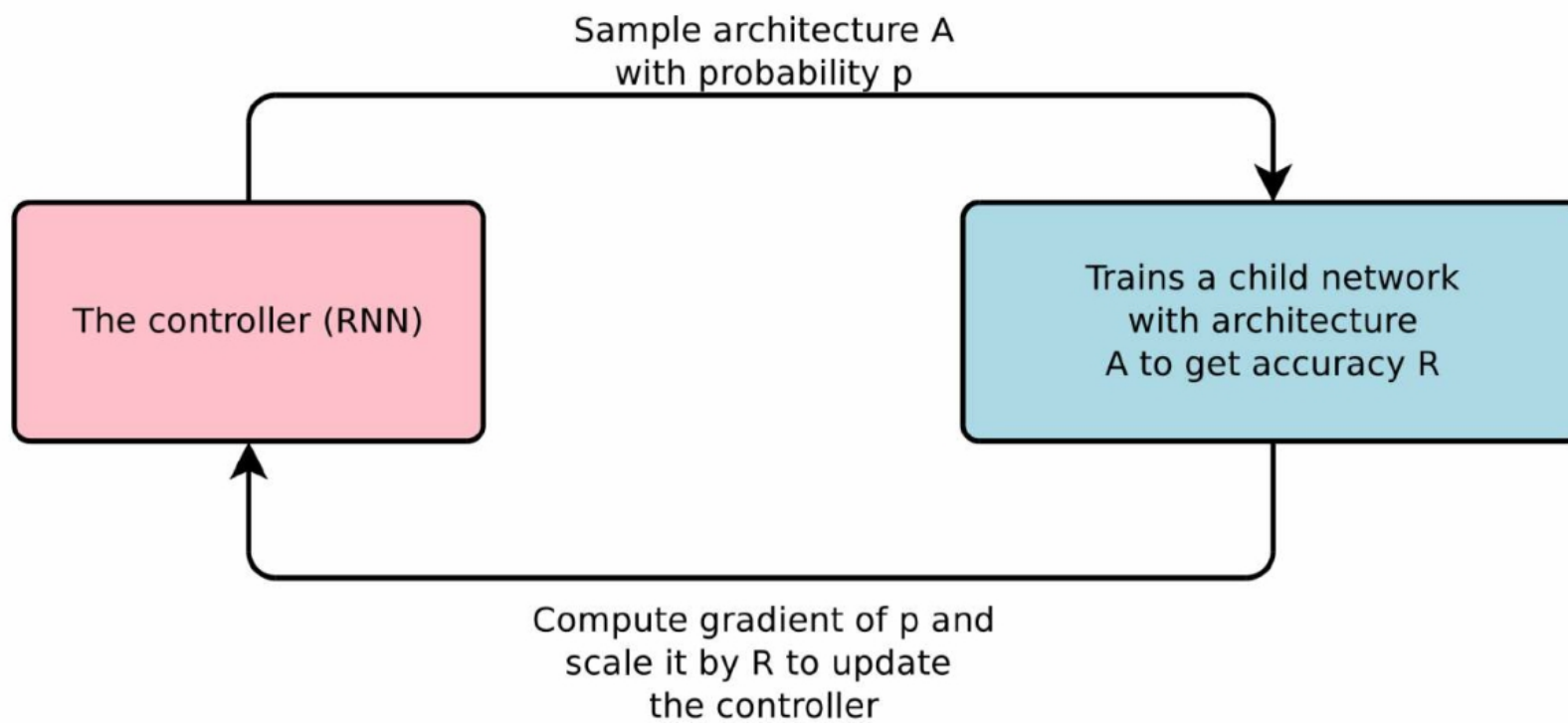
Greater need for specialized engineers

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

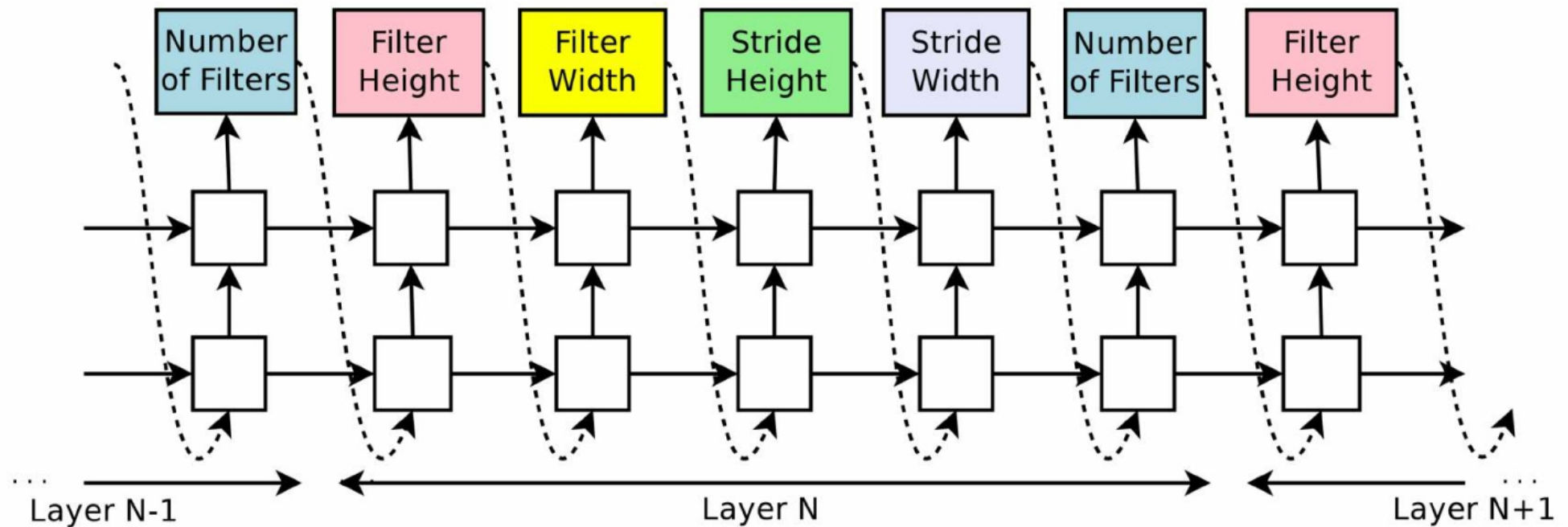
AutoML: Learning to Learn



Zoph and Le, *ICLR* 2017.

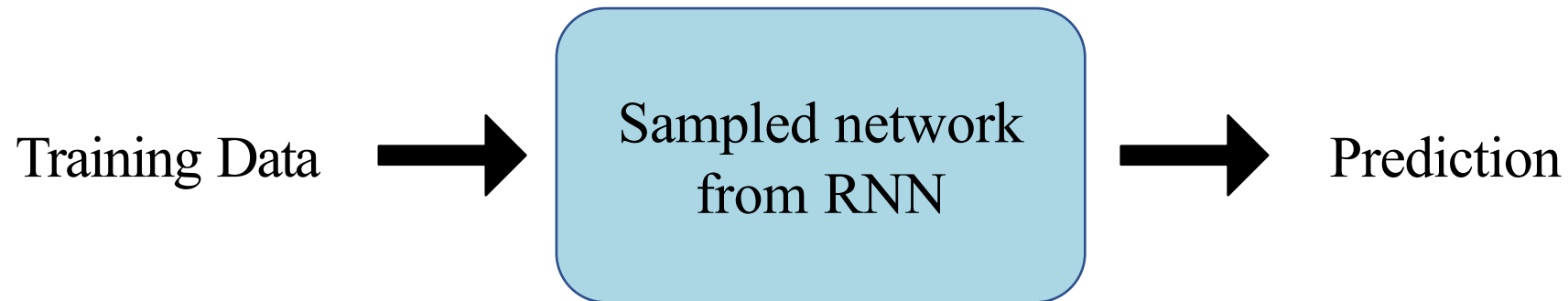
AutoML: Model Controller

At each step, the model samples a brand new network



Zoph and Le, *ICLR* 2017.

AutoML: The Child Network



Compute final accuracy on this dataset.

Update RNN controller based on the accuracy of the child network after training.

AutoML on the Cloud



AutoML Vision^{BETA}

Start with as little as a few dozen photographic samples, and Cloud AutoML will do the rest.



AutoML Natural Language^{BETA}

Automatically predict text categories through either single or multi-label classification.



AutoML Translation^{BETA}

Upload translated language pairs to train your own custom model.