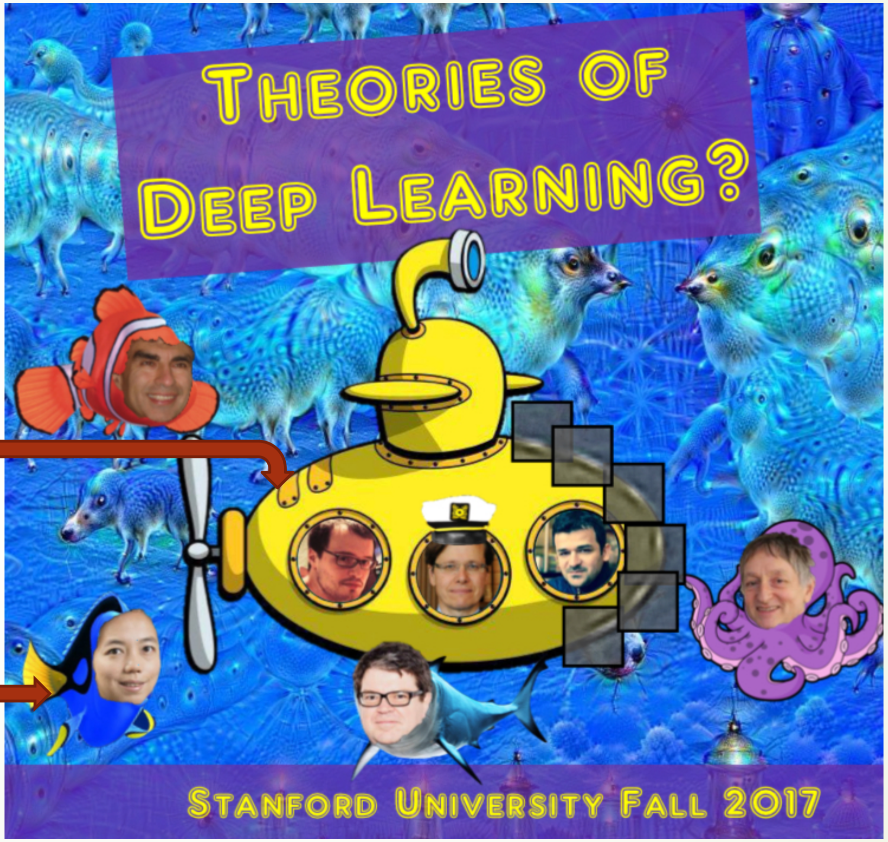
An Introduction to Neural Network and Deep Learning

Yuan YAO
HKUST

Acknowledgement

https://stats385.github.io/

http://cs231n.github.io/



A following-up course at HKUST: https://deeplearning-math.github.io/

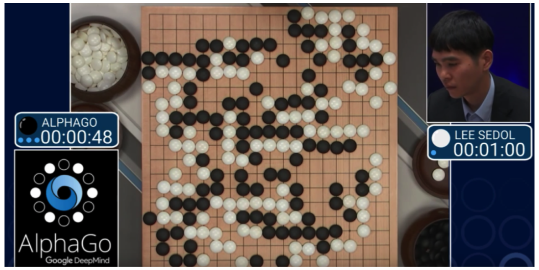
Some reference books

- Deep Learning with Python, Manning Publications 2017
  - by François Chollet
  - https://www.manning.com/books/deep-learning-with-python?a_aid=keras&a_bid=76564dff
- Deep Learning, MIT Press 2016
  - By Ian Goodfellow, Yoshua Bengio, and Aaron Courville,
  - http://www.deeplearningbook.org/
- Many other public resources

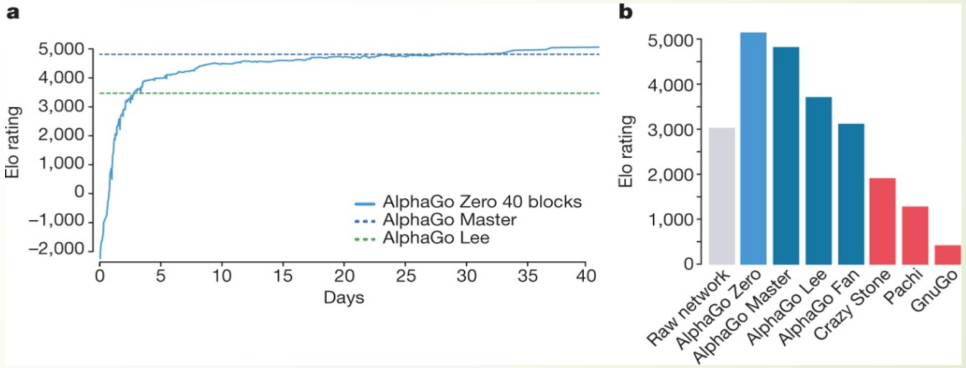
The Tsunami of Deep Learning

Reaching Human Performance Level in Games

Deep Blue in 1997



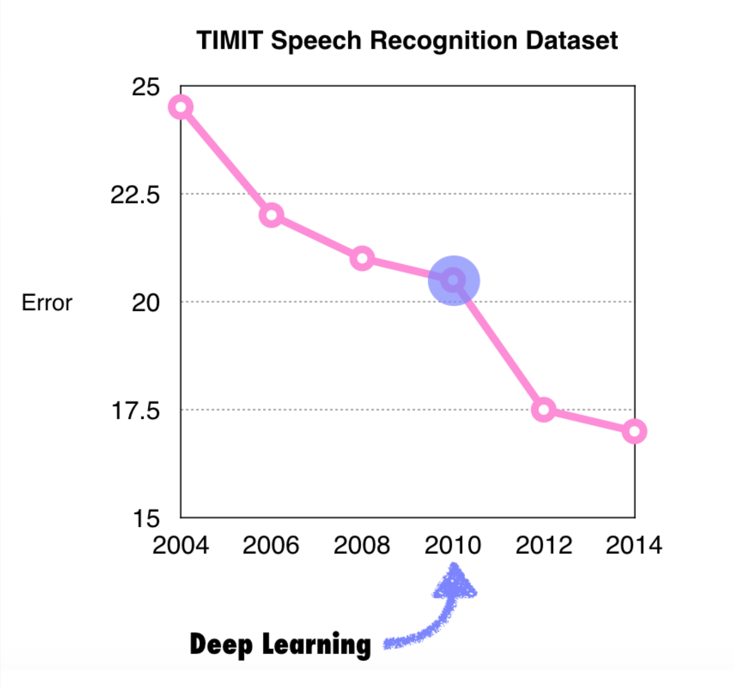
AlphaGo "LEE" 2016



AlphaGo "ZERO" D Silver *et al.* *Nature* **550,** 354–359 (2017) doi:10.1038/nature24270

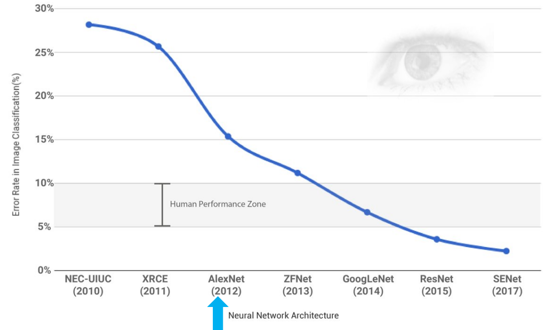
Speech Recognition & Computer Vision

Speech Recognition: TIMIT



Computer Vision: ImageNet

- ImageNet (subset):
  - 1.2 million training images
  - 100,000 test images
  - 1000 classes
- ImageNet large-scale visual recognition Challenge

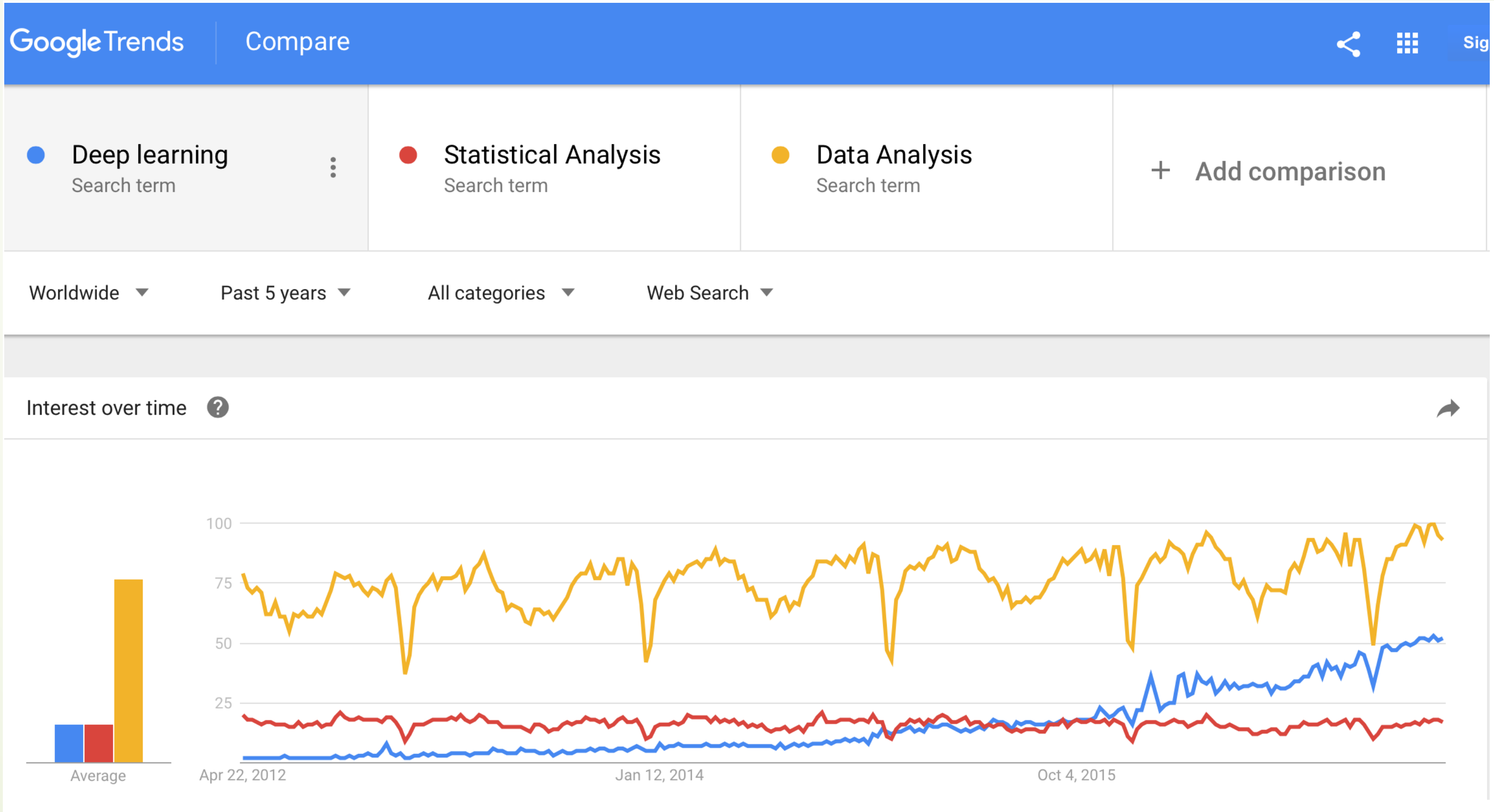


source: https://www.linkedin.com/pulse/must-read-path-breaking-papers-image-classification-muktabh-mayank

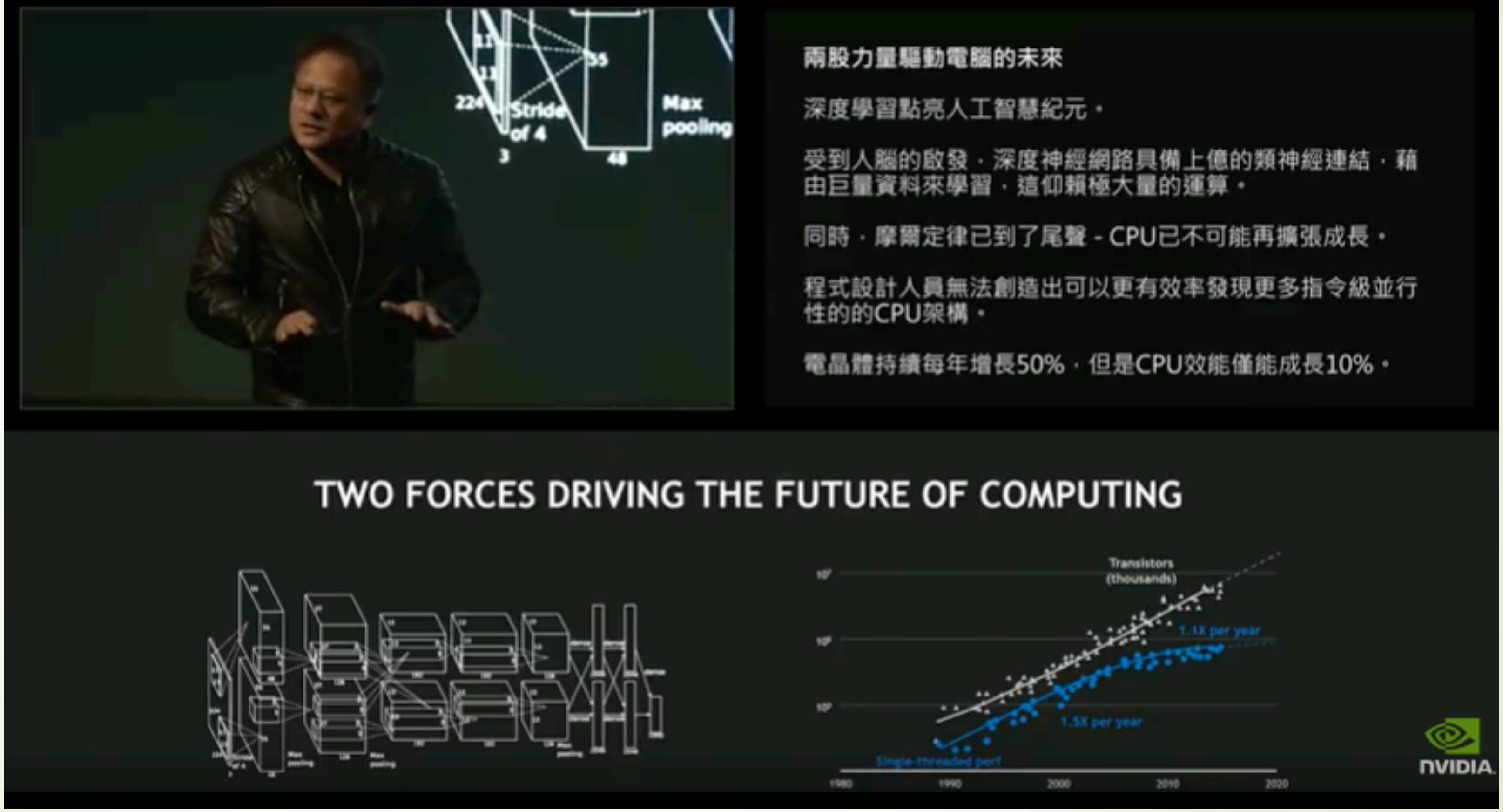
Deep Learning

Growth of Deep Learning

'Deep Learning' is coined by Hinton et al. in their Restricted Boltzman Machine paper, *Science* 2006, not yet popular until championing ImageNet competitions.



"We're at the beginning of a new day…
This is the beginning of the AI revolution."
— Jensen Huang, GTC Taiwan 2017



New Moore's Laws

CS231n attendance

Andrej Karpathy @karpathy
Follow

Came to visit first class of @cs231n at Stanford. 2015: 150 students, 2016: 350, this year: 750. #aiinterestsingularity

12:11 PM - 4 Apr 2017

155 Retweets **623** Likes

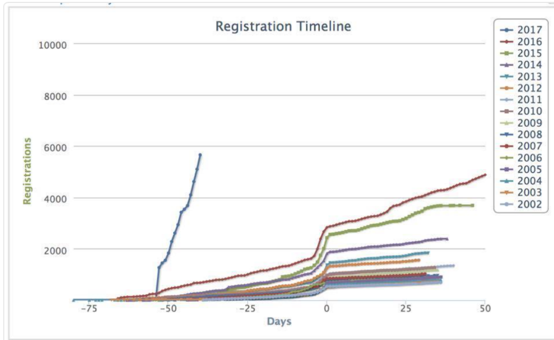
19 155 623

michael_nielsen @michael_nielsen · Apr 4
Replying to @karpathy @cs231n
Faster than Moore's Law. At this rate - doubling each year - in 24 years everyone on Earth will be enrolled :-)

NIPS registrations

Alex Lebrun @lxbrun
Follow

Deep learning hype in one picture (NIPS conference registrations, 2002 through 2017) #nips2017

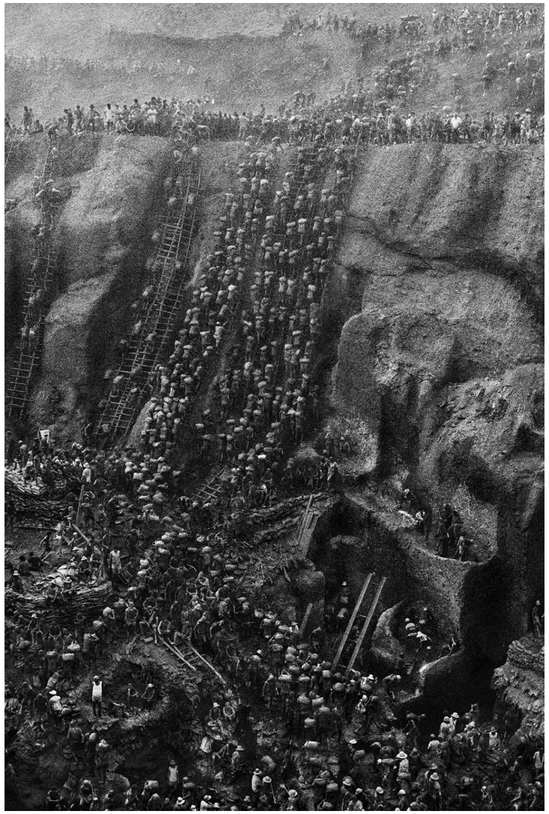


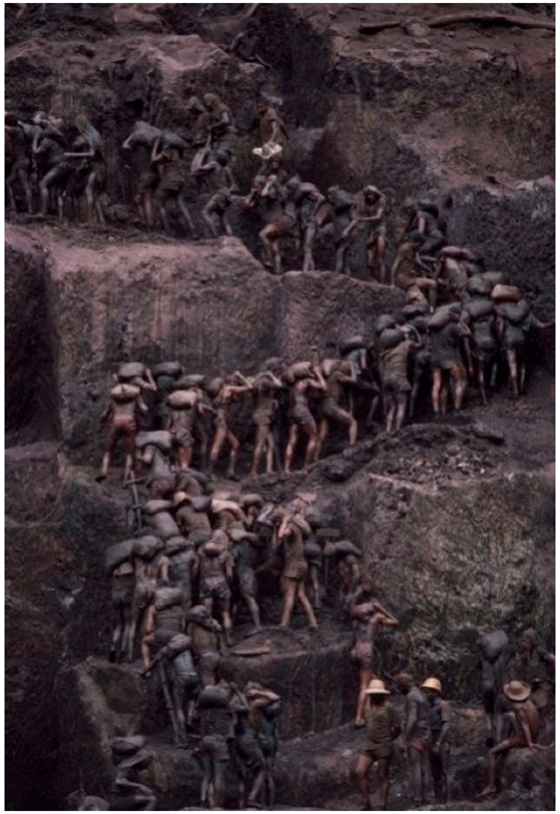
8:20 AM - 15 Sep 2017

758 Retweets **1,005** Likes

20 758 1.0K

Crowdcomputing:
new comers raising the competition record

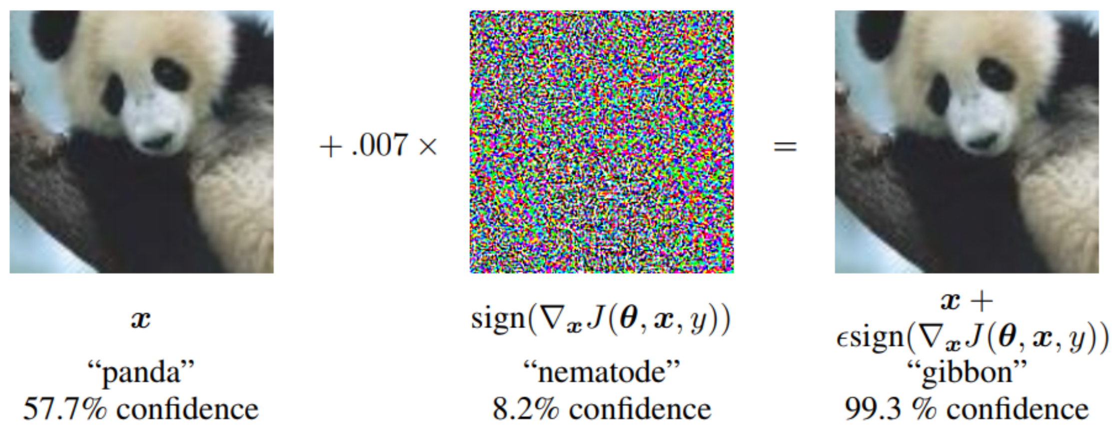




Some Cold Water: Tesla Autopilot Misclassifies Truck as Billboard

Problem: Why? How can you trust a blackbox?

Deep Learning may be fragile in generalization against noise!



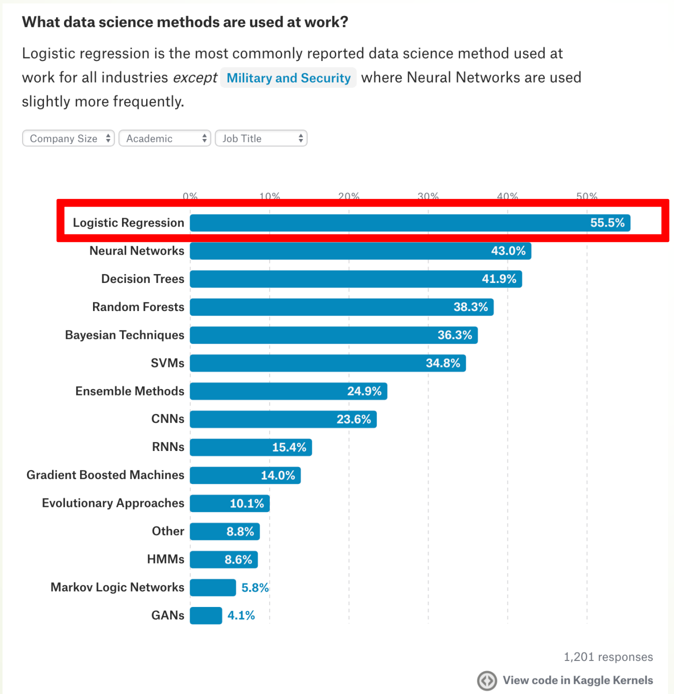
[Goodfellow et al., 2014]

- Small but malicious perturbations can result in severe misclassification
- Malicious examples generalize across different architectures
- What is source of instability?
- Can we robustify network?

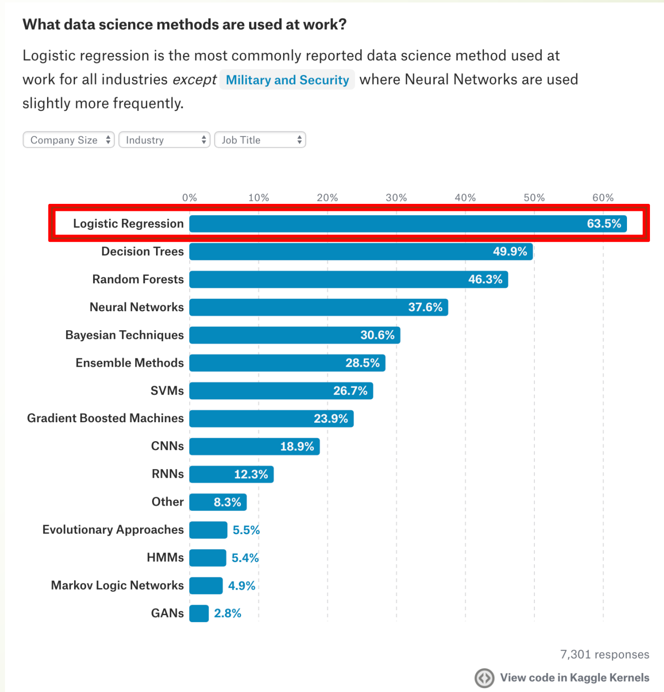
Kaggle survey: Top Data Science Methods

https://www.kaggle.com/surveys/2017

Academic



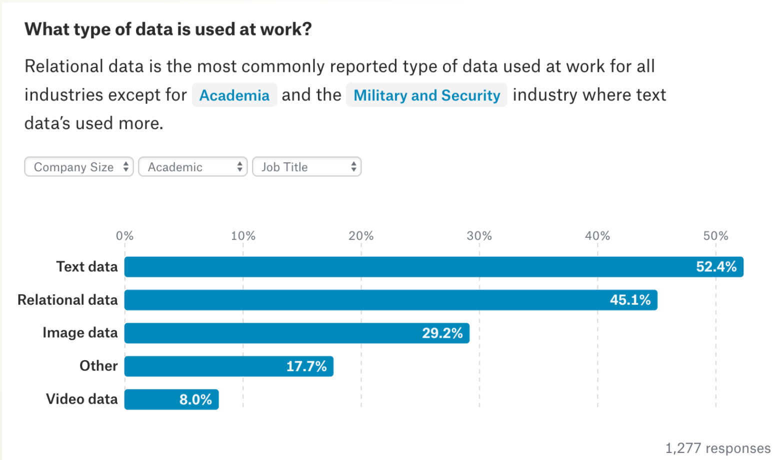
Industry



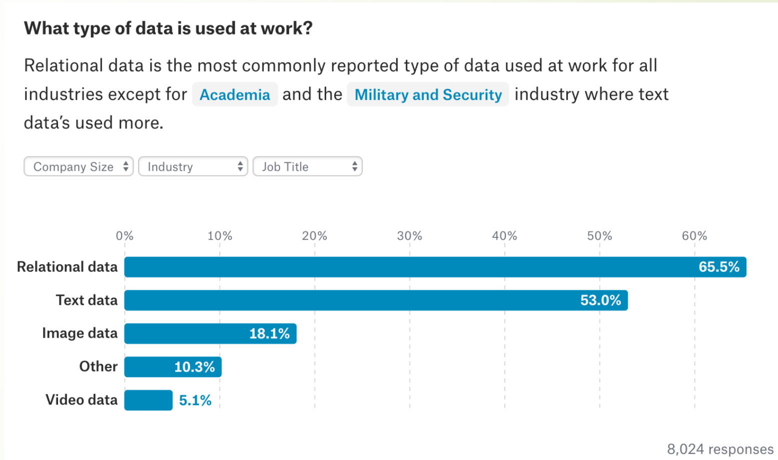
What type of data is used at work?

https://www.kaggle.com/surveys/2017

Academic



Industry



What’s wrong with deep learning?

Ali Rahimi NIPS’17: Machine (deep) Learning has become **alchemy**.
https://www.youtube.com/watch?v=ORHFOnaEzPc

Yann LeCun CVPR’15, invited talk: **What’s wrong with deep learning?**
One important piece: **missing some theory**!

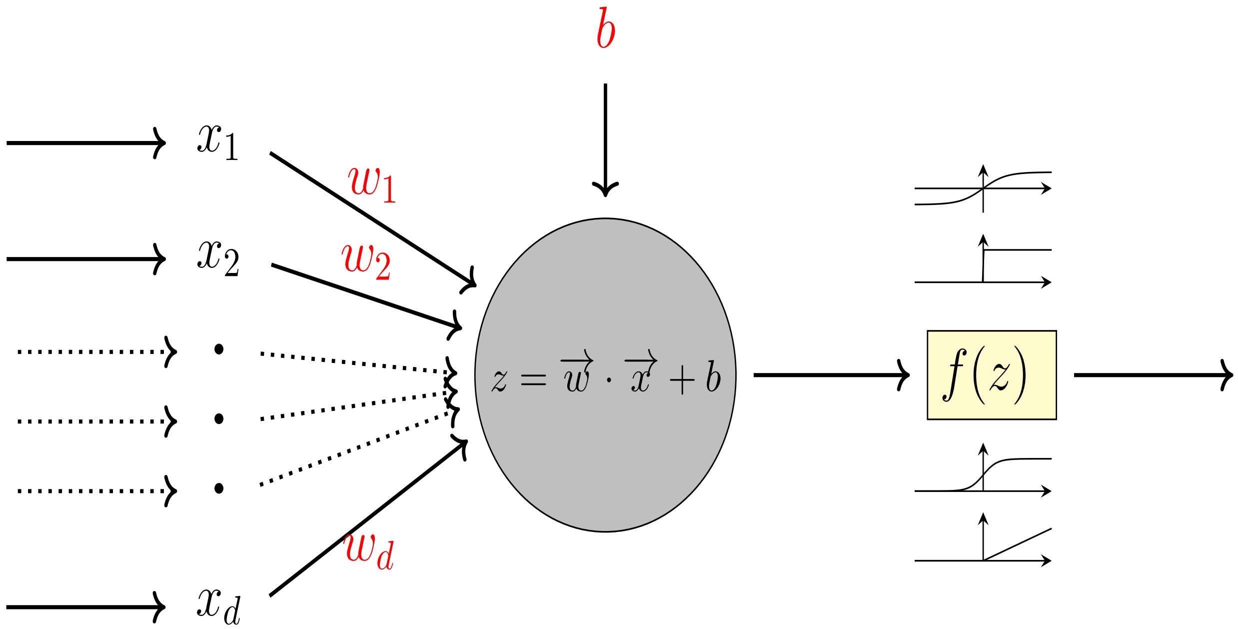
http://techtalks.tv/talks/whats-wrong-with-deep-learning/61639/

We have to know what we are doing…

A Brief History of Neural Networks

Perceptron: single-layer

- Invented by Frank Rosenblatt (1957)



The Perceptron Algorithm

$$\ell(w) = -\sum_{i \in \mathcal{M}_w} y_i \langle w, \mathbf{x}_i \rangle, \quad \mathcal{M}_w = \{i : y_i \langle \mathbf{x}_i, w \rangle < 0, y_i \in \{-1, 1\}\}.$$

The Perceptron Algorithm is a *Stochastic Gradient Descent* method (Robbins–Monro 1950; Kiefer-Wolfowitz 1951) :

$$\begin{aligned} w_{t+1} &= w_t - \eta_t \nabla_i \ell(w) \\ &= \begin{cases} w_t - \eta_t y_i \mathbf{x}_i, & \text{if } y_i w_t^T \mathbf{x}_i < 0, \\ w_t, & \text{otherwise.} \end{cases} \end{aligned}$$

Finite Stop of Perceptron for Separable Data

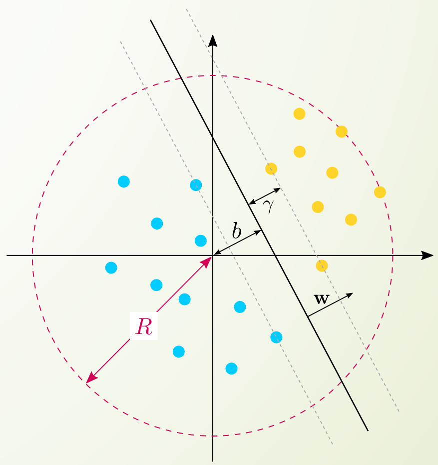
The perceptron convergence theorem was proved by Block (1962) and Novikoff (1962). The following version is based on that in Cristianini and Shawe-Taylor (2000).

Theorem 1 (Block, Novikoff). *Let the training set $S = \{(\mathbf{x}_1, t_1), \ldots, (\mathbf{x}_n, t_n)\}$ be contained in a sphere of radius R about the origin. Assume the dataset to be linearly separable, and let $\mathbf{w}_{\text{opt}}$, $\|\mathbf{w}_{\text{opt}}\| = 1$, define the hyperplane separating the samples, having functional margin $\gamma > 0$. We initialise the normal vector as $\mathbf{w}_0 = \mathbf{0}$. The number of updates, k, of the perceptron algorithms is then bounded by*

$$k \leq \left(\frac{2R}{\gamma}\right)^2. \tag{10}$$

Input ball: $R = \max_i \|\mathbf{x}_i\|.$

Margin: $\gamma := \min_i y_i f(x_i)$



Proof.

Proof. Though the proof can be done using the augmented normal vector and samples defined in the beginning, the notation will be a lot easier if we introduce a different augmentation: $\hat{\mathbf{w}} = (\mathbf{w}^\intercal, b/R)^\intercal = (w_1, \ldots, w_D, b/R)^\intercal$ and $\hat{\mathbf{x}} = (\mathbf{x}^\intercal, R)^\intercal = (x_1, \ldots, x_D, R)^\intercal$.

Proof (continued, growth of $|w_k|$)

We first derive an upper bound on how fast the normal vector grows. As the hyperplane is unchanged if we multiply $\hat{\mathbf{w}}$ by a constant, we can set $\eta = 1$ without loss of generality. Let $\hat{\mathbf{w}}_{k+1}$ be the updated (augmented) normal vector after the kth error has been observed.

$$\begin{aligned} \|\hat{\mathbf{w}}_{k+1}\|^2 &= (\hat{\mathbf{w}}_k + t_i\hat{\mathbf{x}}_i)^\mathsf{T}(\hat{\mathbf{w}}_k + t_i\hat{\mathbf{x}}_i) && (11)\\ &= \hat{\mathbf{w}}_k^\mathsf{T}\hat{\mathbf{w}}_k + \hat{\mathbf{x}}_i^\mathsf{T}\hat{\mathbf{x}}_i + 2t_i\hat{\mathbf{w}}_k^\mathsf{T}\hat{\mathbf{x}}_i && (12)\\ &= \|\hat{\mathbf{w}}_k\|^2 + \|\hat{\mathbf{x}}_i\|^2 + 2t_i\hat{\mathbf{w}}_k^\mathsf{T}\hat{\mathbf{x}}_i\,. && (13) \end{aligned}$$

Since an update was triggered, we know that $t_i\hat{\mathbf{w}}_k^\mathsf{T}\hat{\mathbf{x}}_i \leq 0$, thus

$$\begin{aligned} \|\hat{\mathbf{w}}_k\|^2 + \|\hat{\mathbf{x}}_i\|^2 + 2t_i\hat{\mathbf{w}}_k^\mathsf{T}\hat{\mathbf{x}}_i &\leq \|\hat{\mathbf{w}}_k\|^2 + \|\hat{\mathbf{x}}_i\|^2 && (14)\\ &= \|\hat{\mathbf{w}}_k\|^2 + (\|\mathbf{x}_i\|^2 + R^2) && (15)\\ &\leq \|\hat{\mathbf{w}}_k\|^2 + 2R^2\,. && (16) \end{aligned}$$

This implies that $\|\hat{\mathbf{w}}_k\|^2 \leq 2kR^2$, thus

$$\|\hat{\mathbf{w}}_{k+1}\|^2 \leq 2(k+1)R^2\,. \qquad (17)$$

Proof (continued, projection on w_{opt})

We then proceed to show how the inner product between an update of the normal vector and $\hat{\mathbf{w}}_{\text{opt}}$ increase with each update:

$$\begin{aligned}
\hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{w}}_{k+1} &= \hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{w}}_k + t_i \hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{x}}_i && (18) \\
&\geq \hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{w}}_k + \gamma && (19) \\
&\geq (k+1)\gamma\,, && (20)
\end{aligned}$$

since $\hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{w}}_k \geq k\gamma$. We therefore have

$$k^2\gamma^2 \leq (\hat{\mathbf{w}}_{\text{opt}}^{\mathsf{T}} \hat{\mathbf{w}}_k)^2 \leq \|\hat{\mathbf{w}}_{\text{opt}}\|^2 \|\hat{\mathbf{w}}_k\|^2 \leq 2kR^2 \|\hat{\mathbf{w}}_{\text{opt}}\|^2\,, \tag{21}$$

where we have made use of the Cauchy-Schwarz inequality. As $k^2\gamma^2$ grows faster than $2kR^2$, Eq. (21) can hold if and only if

$$k \leq 2\|\hat{\mathbf{w}}_{\text{opt}}\|^2 \frac{R^2}{\gamma^2}\,. \tag{22}$$

Proof (continued, combined bounds)

As $b \leq R$, we can rewrite the norm of the normal vector:

$$\|\hat{\mathbf{w}}_{\text{opt}}\|^2 = \|\mathbf{w}_{\text{opt}}\|^2 + \frac{b^2}{R^2} \leq \|\mathbf{w}_{\text{opt}}\|^2 + 1 = 2\,. \tag{23}$$

The bound on k now becomes

$$k \leq 4\frac{R^2}{\gamma^2} = \left(\frac{2R}{\gamma}\right)^2, \tag{24}$$

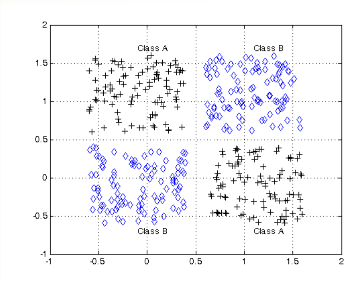
which therefore bounds the number of updates necessary to find the separating hyperplane. □

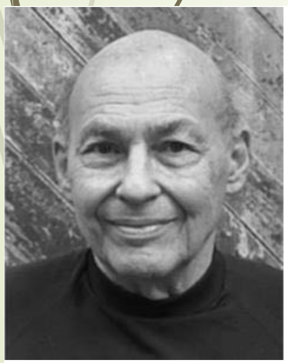
Locality or Sparsity of Computation

Minsky and Papert, 1969

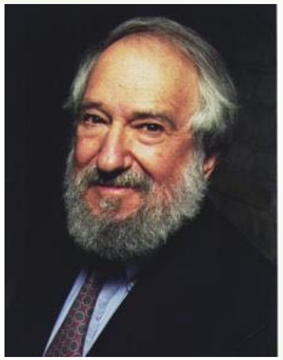
Perceptron can't do **XOR** classification

Perceptron needs infinite global information to compute **connectivity**





Marvin Minsky

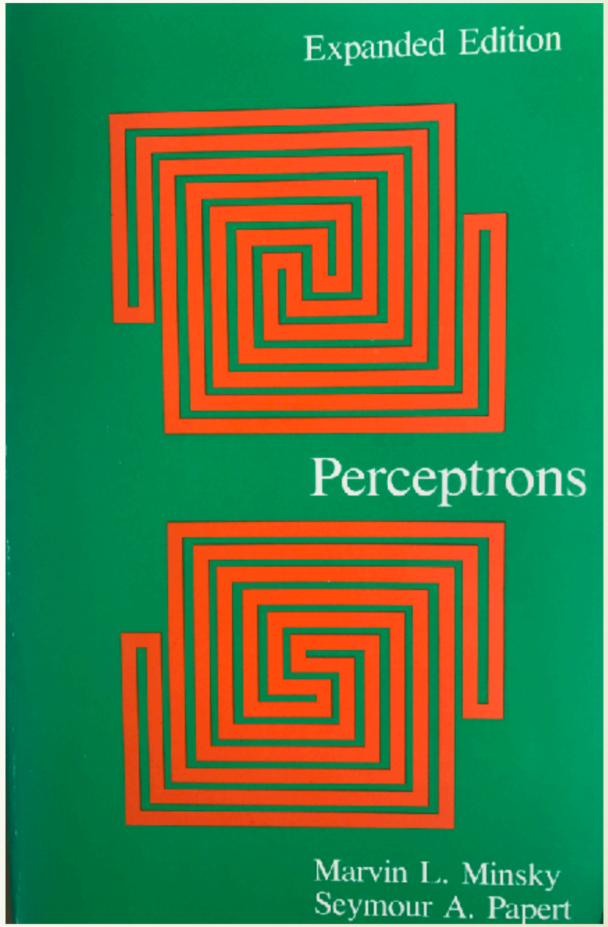


Seymour Papert

Locality or **Sparsity** is important:

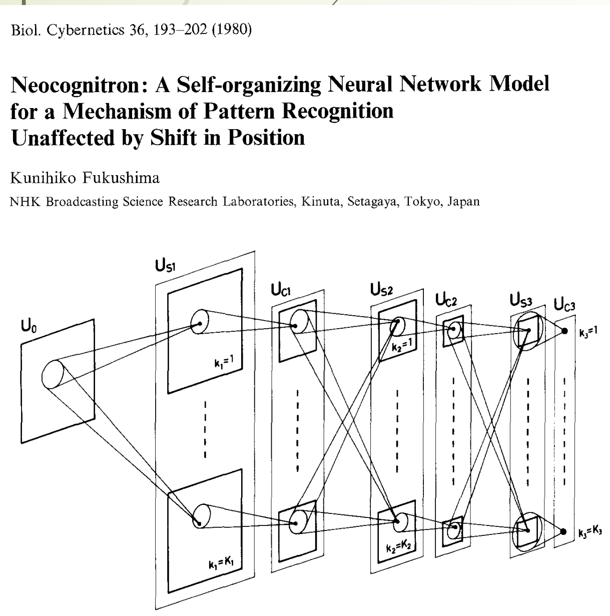
Locality in time?

Locality in space?



Convolutional Neural Networks: shift invariances and locality

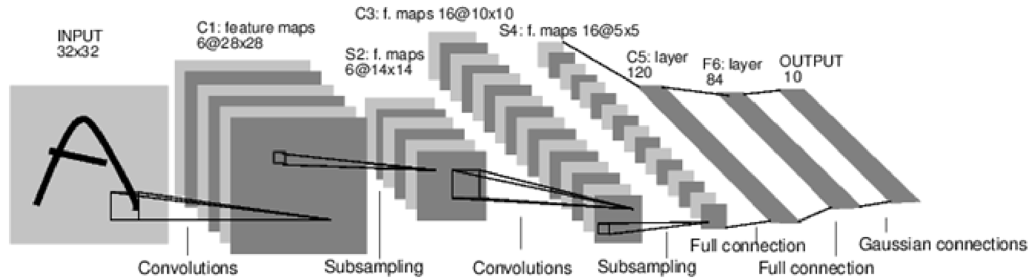
- Can be traced to *Neocognitron* of Kunihiko Fukushima (1979)
- Yann LeCun combined convolutional neural networks with back propagation (1989)
- Imposes **shift invariance** and **locality** on the weights
- Forward pass remains similar
- Backpropagation slightly changes – need to sum over the gradients from all spatial positions


Biol. Cybernetics 36, 193–202 (1980)

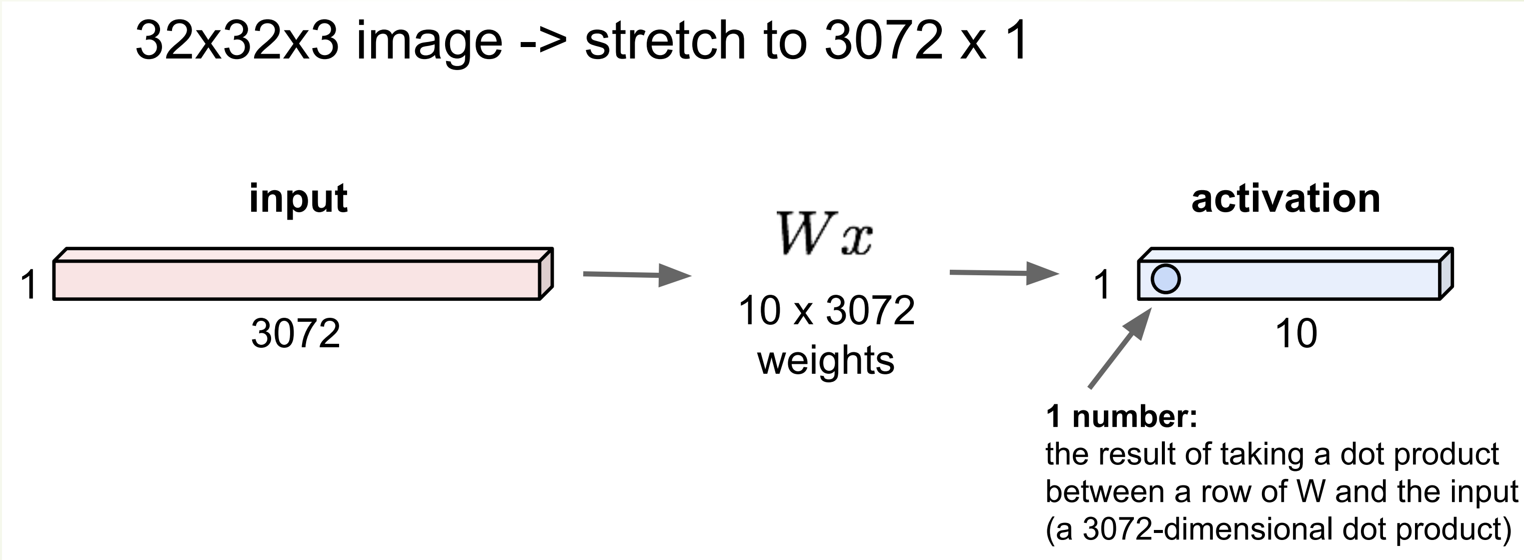
Neocognitron: A Self-organizing Neural Network Model for a Mechanism of Pattern Recognition Unaffected by Shift in Position

Kunihiko Fukushima

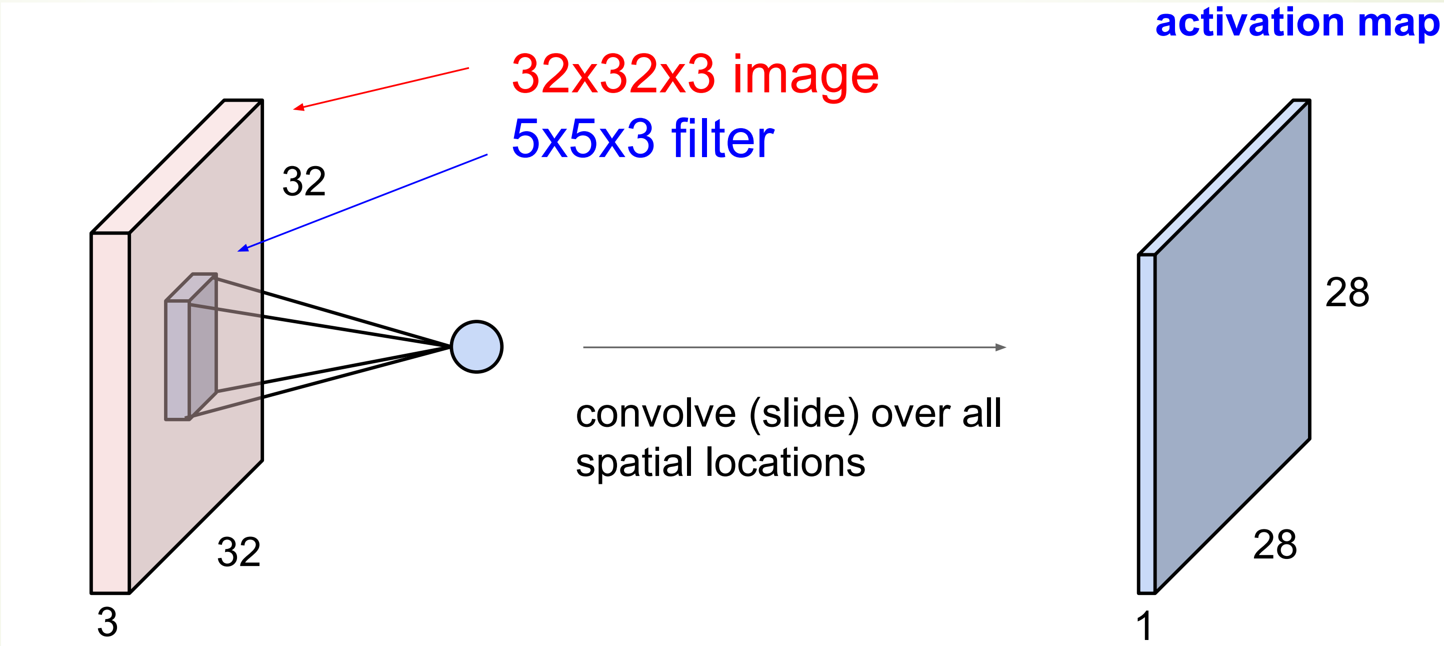
NHK Broadcasting Science Research Laboratories, Kinuta, Setagaya, Tokyo, Japan



Fully Connected Layer



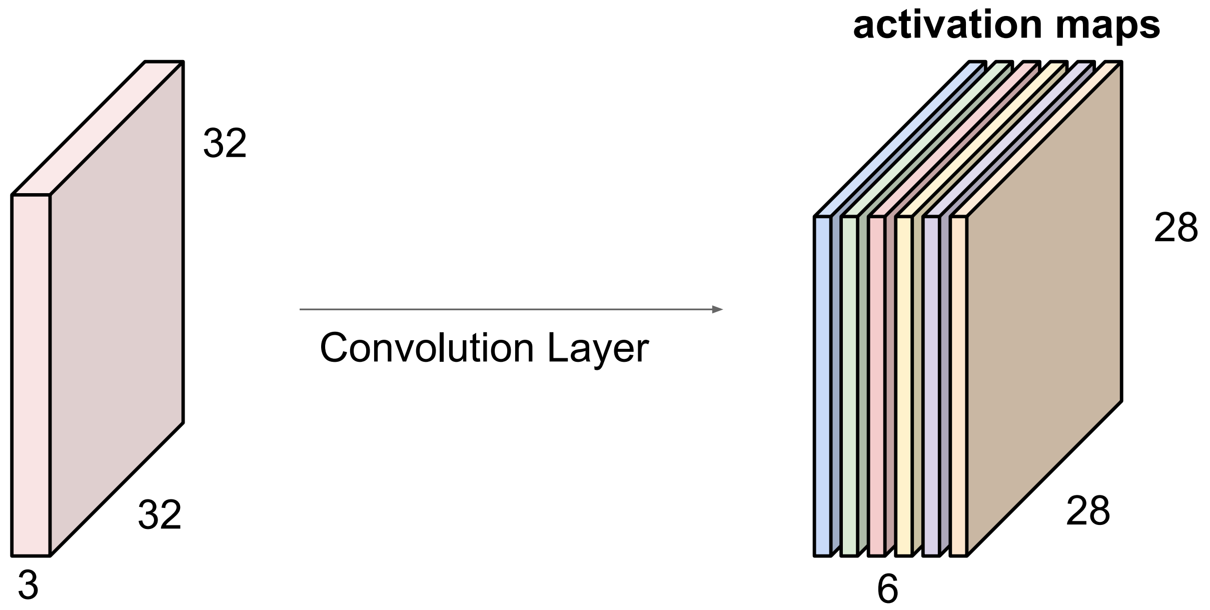
Convolution Layer: a first (blue) filter



Convolution Layer: a second (green) filter

Convolution Layer

For example, if we had 6 5x5 filters, we'll get 6 separate activation maps:



We stack these up to get a "new image" of size 28x28x6!

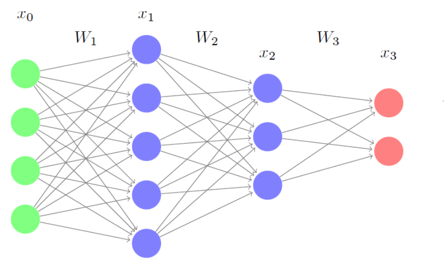
Multilayer Perceptrons (MLP) and Back-Propagation (BP) Algorithms

Rumelhart, Hinton, Williams (1986)
Learning representations by back-propagating errors, Nature, 323(9): 533-536

BP algorithms as **stochastic gradient descent** algorithms (**Robbins–Monro 1950; Kiefer-Wolfowitz 1951**) with Chain rules of Gradient maps

MLP classifies **XOR**, but the global hurdle on topology (connectivity) computation still exists

NATURE VOL. 323 9 OCTOBER 1986 — LETTERS TO NATURE — 533



Learning representations by back-propagating errors

David E. Rumelhart*, Geoffrey E. Hinton† & Ronald J. Williams*

* Institute for Cognitive Science, C-015, University of California, San Diego, La Jolla, California 92093, USA
† Department of Computer Science, Carnegie-Mellon University, Pittsburgh, Philadelphia 15213, USA

We describe a new learning procedure, back-propagation, for networks of neurone-like units. The procedure repeatedly adjusts the weights of the connections in the network so as to minimize a measure of the difference between the actual output vector of the net and the desired output vector. As a result of the weight adjustments, internal 'hidden' units which are not part of the input or output come to represent important features of the task domain, and the regularities in the task are captured by the interactions of these units. The ability to create useful new features distinguishes back-propagation from earlier, simpler methods such as the perceptron-convergence procedure[1].

There have been many attempts to design self-organizing neural networks. The aim is to find a powerful synaptic modification rule that will allow an arbitrarily connected neural network to develop an internal structure that is appropriate for a particular task domain. The task is specified by giving the desired state vector of the output units for each state vector of the input units. If the input units are directly connected to the output units it is relatively easy to find learning rules that iteratively adjust the relative strengths of the connections so as to progressively reduce the difference between the actual and desired output vectors[2]. Learning becomes more interesting but more difficult when we introduce hidden units whose actual or desired states are not specified by the task. (In perceptrons, there are 'feature analysers' between the input and output that are not true hidden units because their input connections are fixed by hand, so their states are completely determined by the input vector: they do not learn representations.) The learning procedure must decide under what circumstances the hidden units should be active in order to help achieve the desired input–output behaviour. This amounts to deciding what these units should represent. We demonstrate that a general purpose and relatively simple procedure is powerful enough to construct appropriate internal representations.

The simplest form of the learning procedure is for layered networks which have a layer of input units at the bottom; any number of intermediate layers; and a layer of output units at the top. Connections within a layer or from higher to lower layers are forbidden, but connections can skip intermediate layers. An input vector is presented to the network by setting the states of the input units. Then the states of the units in each layer are determined by applying equations (1) and (2) to the connections coming from lower layers. All units within a layer have their states set in parallel, but different layers have their states set sequentially, starting at the bottom and working upwards until the states of the output units are determined.

The total input, x_j, to unit j is a linear function of the outputs, y_i, of the units that are connected to j and of the weights, w_{ji}, on these connections

$$x_j = \sum_i y_i w_{ji} \qquad (1)$$

Units can be given biases by introducing an extra input to each unit which always has a value of 1. The weight on this extra input is called the bias and is equivalent to a threshold of the opposite sign. It can be treated just like the other weights.

A unit has a real-valued output, y_j, which is a non-linear function of its total input

$$y_j = \frac{1}{1+e^{-x_j}} \qquad (2)$$

† To whom correspondence should be addressed

BP Algorithm: Forward Pass

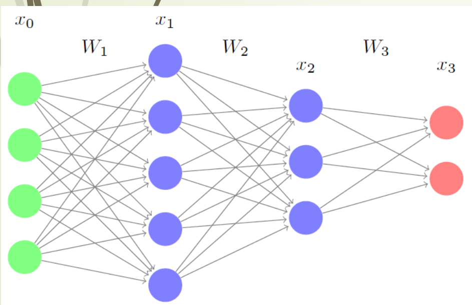
- Cascade of repeated [linear operation followed by coordinatewise nonlinearity]'s
- Nonlinearities: sigmoid, hyperbolic tangent, (recently) ReLU.

Algorithm 1 Forward pass

Input: x_0

Output: x_L

for $\ell = 1$ to L **do**
    $x_\ell = f_\ell(W_\ell x_{\ell-1} + b_\ell)$
end for



BP algorithm = Gradient Descent Method

- Training examples $\{x_0^i\}_{i=1}^n$ and labels $\{y^i\}_{i=1}^n$
- Output of the network $\{x_L^i\}_{i=1}^m$
- Objective

$$J(\{W_l\}, \{b_l\}) = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{2} \|y^i - x_L^i\|_2^2 \qquad (1)$$

Other losses include cross-entropy, logistic loss, exponential loss, etc.

- Gradient descent

$$W_l = W_l - \eta \frac{\partial J}{\partial W_l}$$

$$b_l = b_l - \eta \frac{\partial J}{\partial b_l}$$

In practice: use Stochastic Gradient Descent (SGD)

Derivation of BP: Lagrangian Multiplier

LeCun et al. 1988

Given n training examples $(I_i, y_i) \equiv$ (input,target) and L layers

- Constrained optimization

$$\min_{W,x} \quad \sum_{i=1}^{n} \|x_i(L) - y_i\|_2$$

subject to $x_i(\ell) = f_\ell\Big[W_\ell x_i(\ell - 1)\Big],$

$$i = 1, \ldots, n, \quad \ell = 1, \ldots, L, \; x_i(0) = I_i$$

- Lagrangian formulation (Unconstrained)

$$\min_{W,x,B} \mathcal{L}(W, x, B)$$

$$\mathcal{L}(W, x, B) = \sum_{i=1}^{n} \Bigg\{ \|x_i(L) - y_i\|_2^2 + \sum_{\ell=1}^{L} B_i(\ell)^T \Big(x_i(\ell) - f_\ell\Big[W_\ell x_i(\ell - 1)\Big]\Big) \Bigg\}$$

http://yann.lecun.com/exdb/publis/pdf/lecun-88.pdf

back-propagation – derivation

- $\frac{\partial \mathcal{L}}{\partial B}$

Forward pass

$$x_i(\ell) = f_\ell\Big[\underbrace{W_\ell x_i\,(\ell-1)}_{A_i(\ell)}\Big] \quad \ell = 1,\dots,L, \quad i = 1,\dots,n$$

- $\frac{\partial \mathcal{L}}{\partial x}$, $z_\ell = [\nabla f_\ell]B(\ell)$

Backward (adjoint) pass

$$z(L) = 2\nabla f_L\Big[A_i(L)\Big]\,(y_i - x_i(L))$$

$$z_i(\ell) = \nabla f_\ell\Big[A_i(\ell)\Big]W_{\ell+1}^T z_i(\ell+1) \quad \ell = 0,\dots,L-1$$

- $W \leftarrow W + \lambda \frac{\partial \mathcal{L}}{\partial W}$

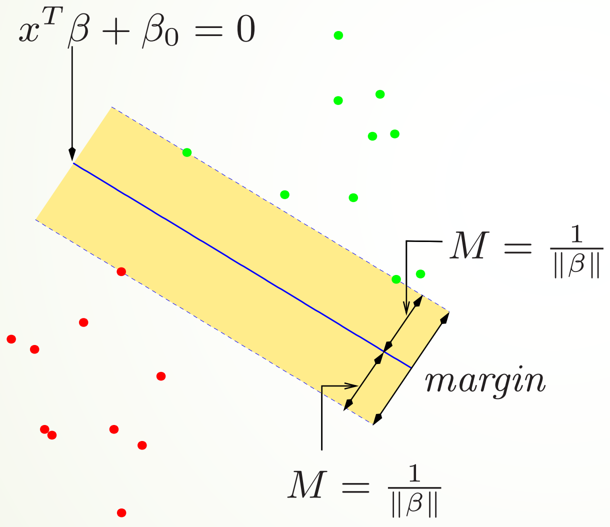
Weight update

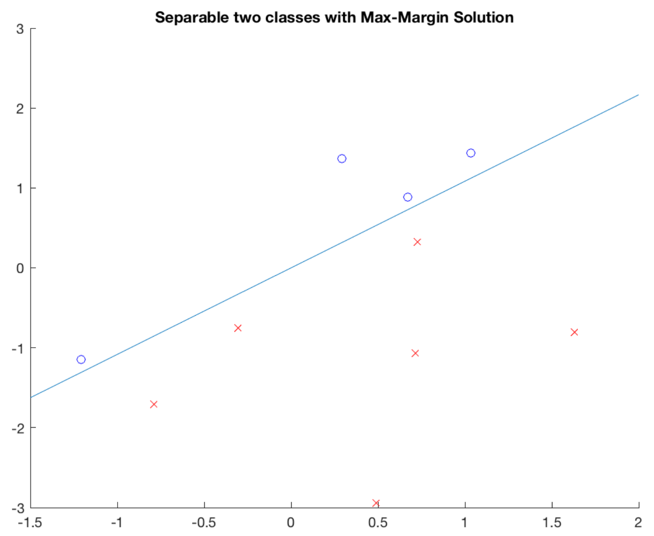
$$W_\ell \leftarrow W_\ell + \lambda \sum_{i=1}^{n} z_i(\ell) x_i^T(\ell-1)$$

Support Vector Machine (Max-Margin Classifier)

$$\text{minimize}_{\beta_0,\beta_1,\ldots,\beta_p} \|\beta\|^2 := \sum_j \beta_j^2$$

$$\text{subject to } y_i(\beta_0 + \beta_1 x_{i1} + \ldots + \beta_p x_{ip}) \geq 1 \text{ for all } i$$

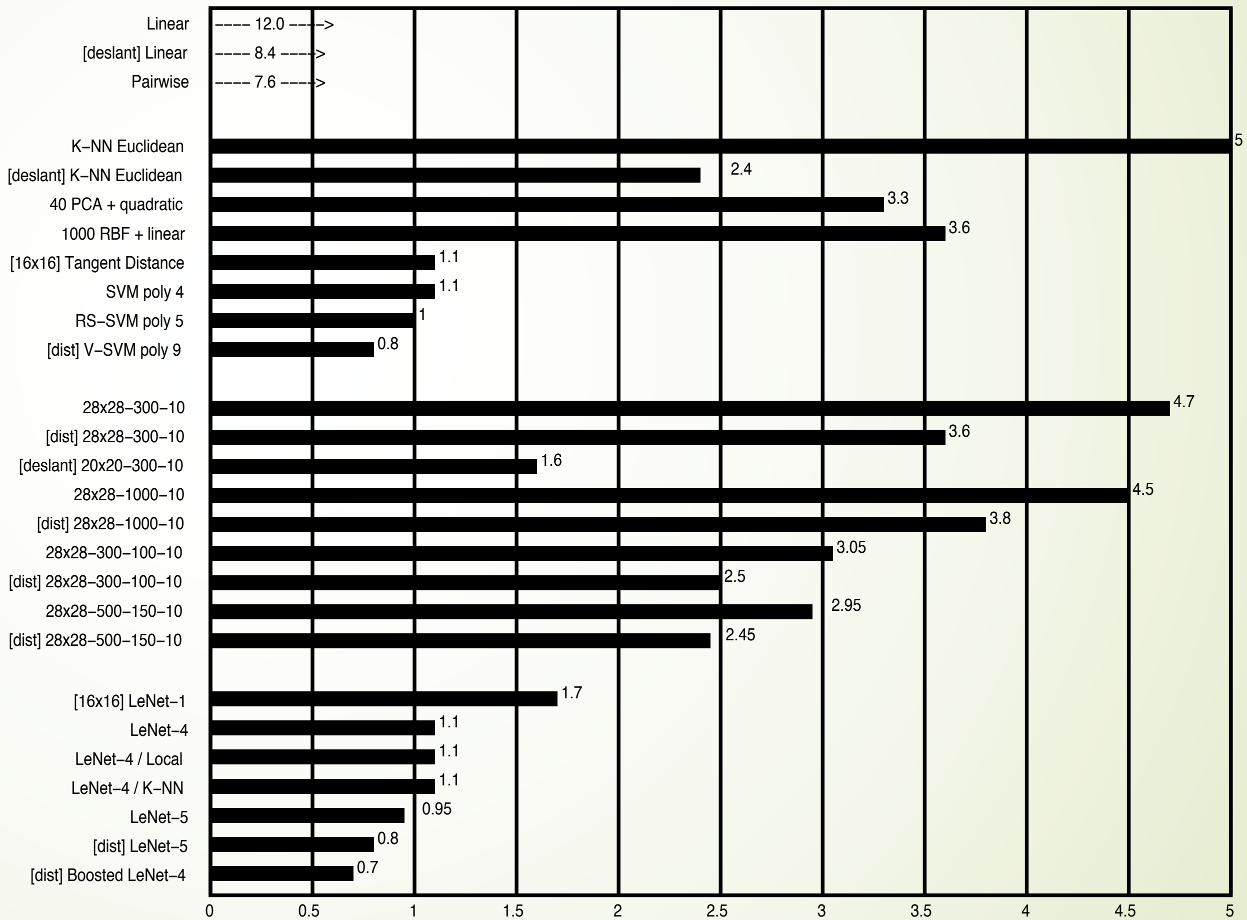




Vladmir Vapnik, 1994

Convex optimization + Reproducing Kernel Hilbert Spaces (Grace Wahba etc.)

MNIST Dataset Test Error: SVM vs. CNN
LeCun et al. 1998

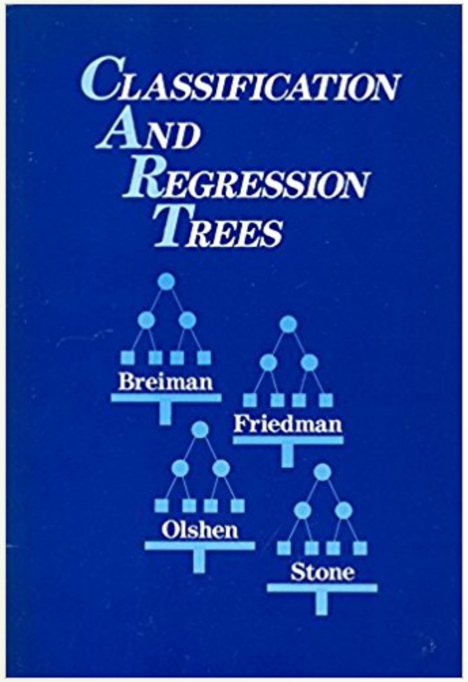


Simple SVM performs as well as Multilayer Convolutional Neural Networks which need careful tuning (LeNets)

Second dark era for NN: 2000s

2000-2010: The Era of SVM, Boosting, … as nights of Neural Networks

Decision Trees and Boosting



- Breiman, Friedman, Olshen, Stone, (1983): CART
- ``The Boosting problem'' (M. Kearns & L. Valiant): **Can a set of weak learners create a single strong learner?** (三个臭皮匠顶个诸葛亮？)
- Breiman (1996): Bagging
- Freund, Schapire (1997): AdaBoost
- Breiman (2001): Random Forests