UPPSALA UNIVERSITET

Machine learning – Block 3

Måns Magnusson
Department of Statistics, Uppsala University

Autumn 2025

UPPSALA UNIVERSITET

This week's lecture

- Feed-Forward Neural Networks
- Regularization of Neural Networks
- Neural Network Optimization

UPPSALA UNIVERSITET

On this weeks assignment

- It can be tricky to get Tensorflow and R to work. Start early and use the zoom sessions.
- Don't run Tensorflow in markdown.

UPPSALA UNIVERSITET

Section 1

Introduction

UPPSALA UNIVERSITET

The Hype: Deep Learning

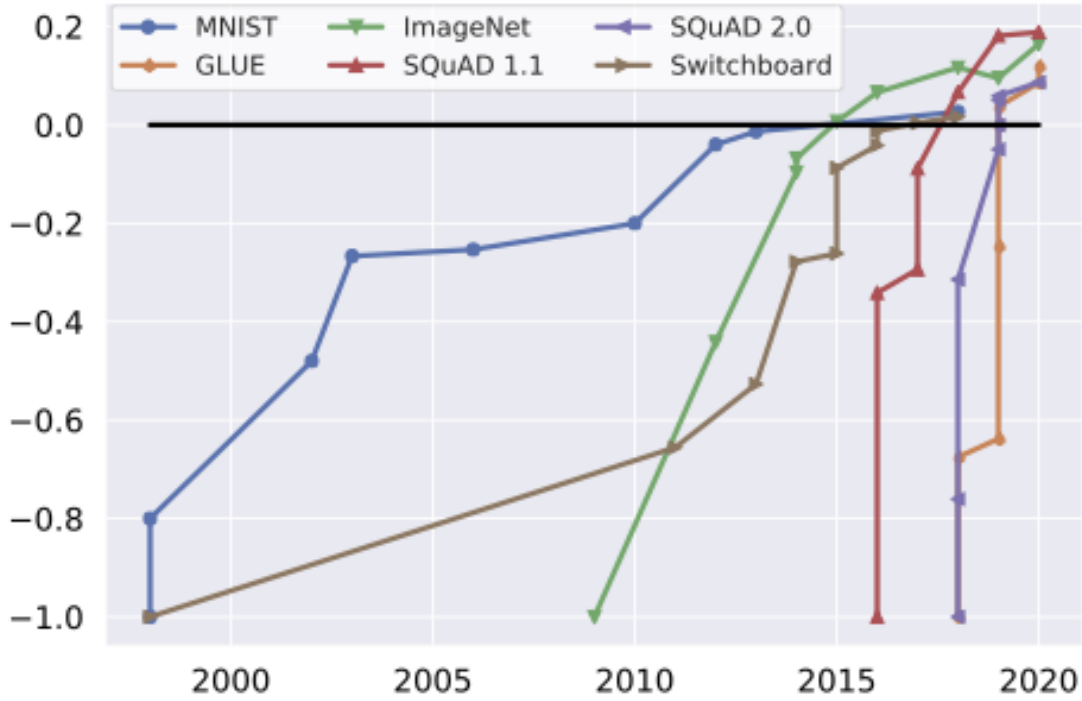


Figure: Benchmark saturation over time for popular benchmarks, normalized with initial performance at mi- nus one and human performance at zero. (Kiela et al., 2021)

UPPSALA UNIVERSITET

The Hype: Large Language Models

- GPT-3 (2020) 175B parameters; breakthrough in general language capabilities.

UPPSALA UNIVERSITET

The Hype: Large Language Models

- GPT-3 (2020) 175B parameters; breakthrough in general language capabilities.
- 2021–2022: Scaling + Instruction Tuning : ChatGPT
  - Models such as GPT-3.5, Gopher, Chinchilla, PaLM.
  - Emergence of instruction-following (ChatGPT)

UPPSALA UNIVERSITET

The Hype: Large Language Models

- GPT-3 (2020) 175B parameters; breakthrough in general language capabilities.
- 2021–2022: Scaling + Instruction Tuning : ChatGPT
  - Models such as GPT-3.5, Gopher, Chinchilla, PaLM.
  - Emergence of instruction-following (ChatGPT)
- 2023: GPT-4 Era
  - Multimodal models (image+text)
  - Open models: LLaMA, Falcon
  - Focus on safety and alignment

UPPSALA UNIVERSITET

The Hype: Large Language Models

- GPT-3 (2020) 175B parameters; breakthrough in general language capabilities.
- 2021–2022: Scaling + Instruction Tuning : ChatGPT
  - Models such as GPT-3.5, Gopher, Chinchilla, PaLM.
  - Emergence of instruction-following (ChatGPT)
- 2023: GPT-4 Era
  - Multimodal models (image+text)
  - Open models: LLaMA, Falcon
  - Focus on safety and alignment
- 2024: Open-Weights Explosion
  - LLaMA-2/3, Mistral, Mixtral (MoE)
  - Efficient inference and training.
  - Training data reached internet-size.

UPPSALA UNIVERSITET

The Hype: Large Language Models

- GPT-3 (2020) 175B parameters; breakthrough in general language capabilities.
- 2021–2022: Scaling + Instruction Tuning : ChatGPT
  - Models such as GPT-3.5, Gopher, Chinchilla, PaLM.
  - Emergence of instruction-following (ChatGPT)
- 2023: GPT-4 Era
  - Multimodal models (image+text)
  - Open models: LLaMA, Falcon
  - Focus on safety and alignment
- 2024: Open-Weights Explosion
  - LLaMA-2/3, Mistral, Mixtral (MoE)
  - Efficient inference and training.
  - Training data reached internet-size.
- 2025: Multimodal Models
  - Native multimodal architectures (audio–vision–text).
  - Agents: reasoning + planning + tool execution.
  - GPT-5 released

UPPSALA UNIVERSITET

The Hype

- Although - (Deep) Neural Networks are not a silver bullet

UPPSALA UNIVERSITET

The Hype

- Although - (Deep) Neural Networks are not a silver bullet
- Remember the Bayes error

UPPSALA UNIVERSITET

The Hype

- Although - (Deep) Neural Networks are not a silver bullet
- Remember the Bayes error
- Sometimes a linear regression (or Random Forest) is enough

UPPSALA UNIVERSITET

Areas of Use

- Supervised learning
- Self-Supervised learning
- Unsupervised learning
- Reinforcement learning

UPPSALA UNIVERSITET

Why and when neural nets?

- Learning feature representations
- Needs a lot of data to learn complex representations (image, text, audio)
- Good for sensor data (high-dimensional)

UPPSALA UNIVERSITET

Why and when neural nets?

- Learning feature representations
- Needs a lot of data to learn complex representations (image, text, audio)
- Good for sensor data (high-dimensional)
- When should we not use neural networks?

UPPSALA UNIVERSITET

Learning Representations

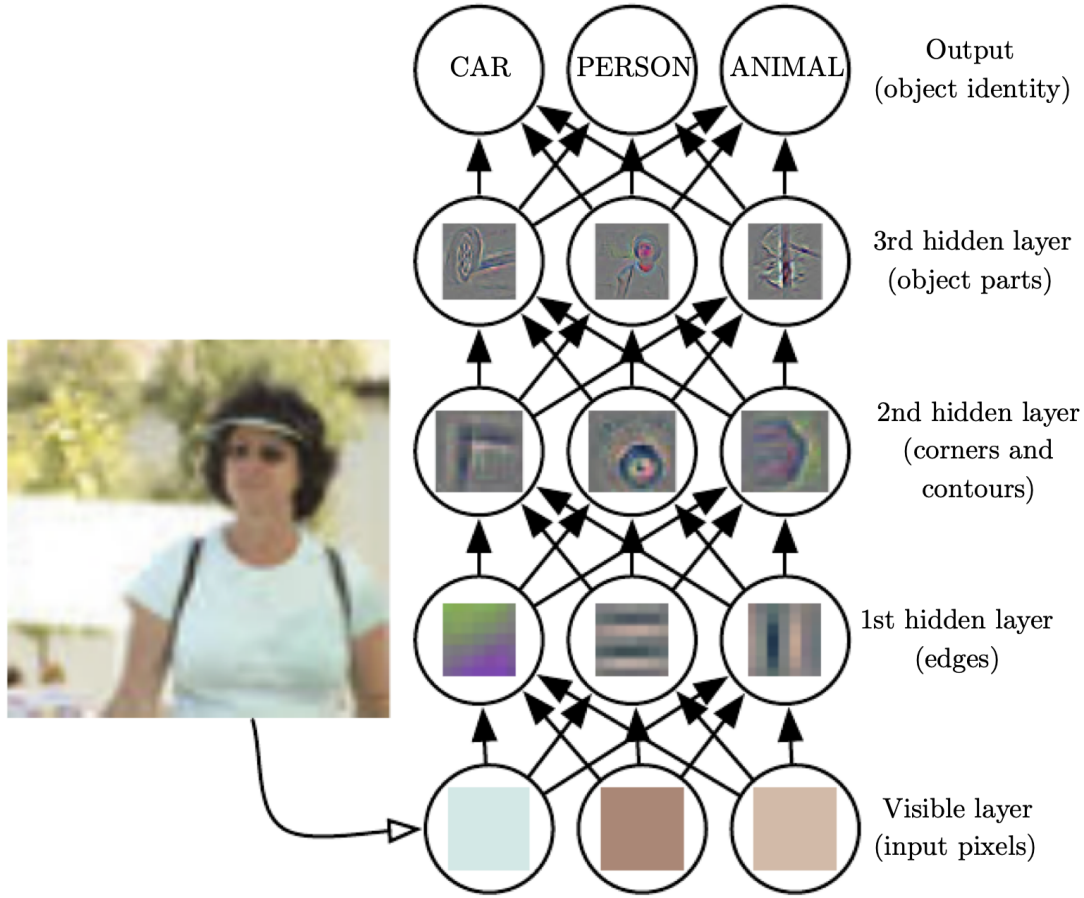


Figure: Learning representations can be crucial (Goodfellow et al, 2017, Fig. 1.2)

UPPSALA UNIVERSITET

Different Network Architectures for Different Purposes

- Different networks for different purposes
  - Feed-Forward Neural Network: Basic building block

UPPSALA UNIVERSITET

Different Network Architectures for Different Purposes

- Different networks for different purposes
  - Feed-Forward Neural Network: Basic building block
  - Convolutional Neural Networks: Computer Vision

UPPSALA UNIVERSITET

Different Network Architectures for Different Purposes

- Different networks for different purposes
  - Feed-Forward Neural Network: Basic building block
  - Convolutional Neural Networks: Computer Vision
  - Transformer Neural Networks: Text/Audio/Vision
  - Diffusion Neural Networks: Image generation

UPPSALA UNIVERSITET

Section 2

Feed-Forward Neural Networks

UPPSALA UNIVERSITET

The Feed-Forward Network

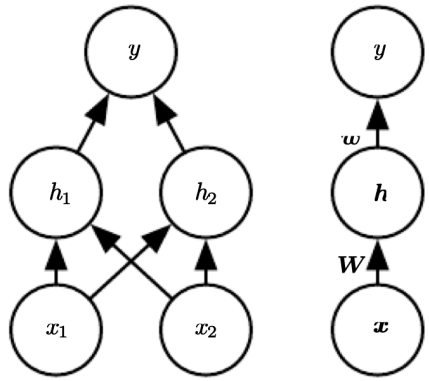


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers

UPPSALA UNIVERSITET

The Feed-Forward Network

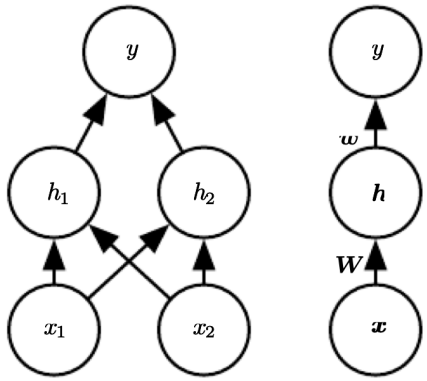


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons

UPPSALA UNIVERSITET

The Feed-Forward Network

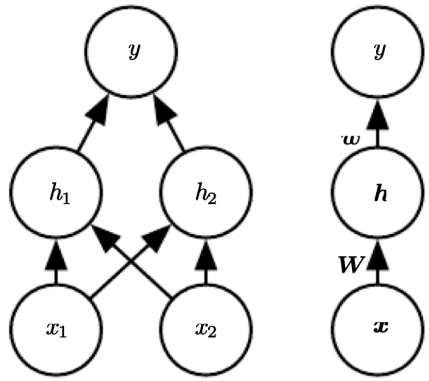


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons, input

UPPSALA UNIVERSITET

The Feed-Forward Network

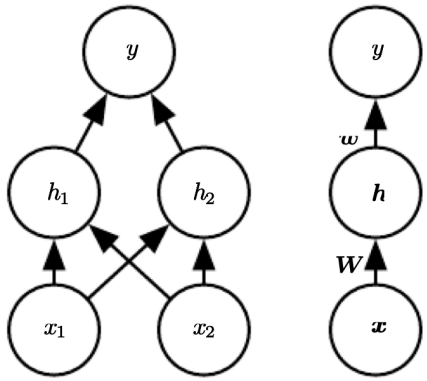


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons, input, output

UPPSALA UNIVERSITET

The Feed-Forward Network

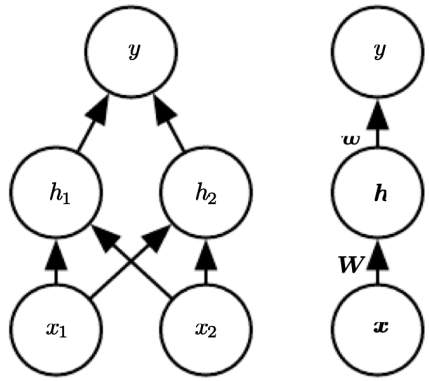


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons, input, output, weights

UPPSALA UNIVERSITET

The Feed-Forward Network

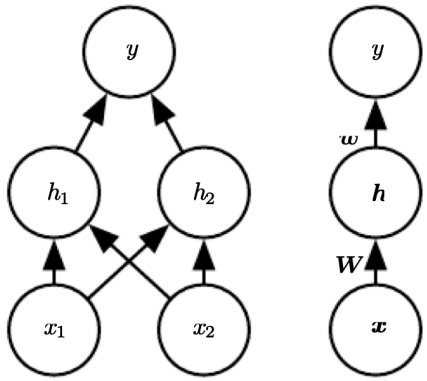


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons, input, output, weights, bias

UPPSALA UNIVERSITET

The Feed-Forward Network

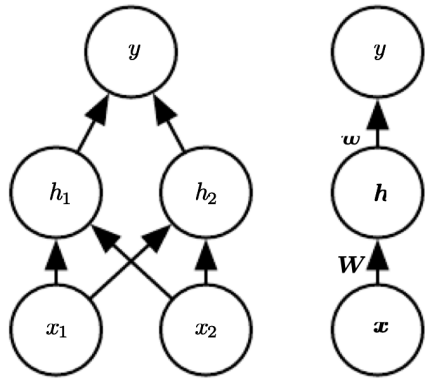


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

Important concepts:

Layers, neurons, input, output, weights, bias, architecture

UPPSALA UNIVERSITET

The Feed-Forward Network

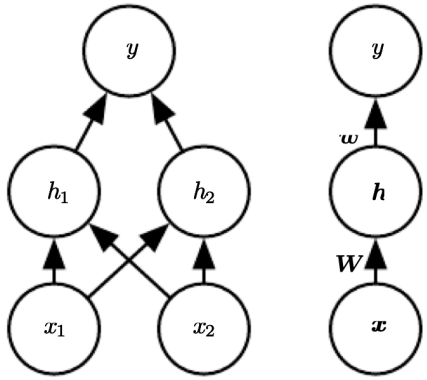


Figure 6.2: An example of a feedforward network, drawn in two different styles. Specifically, this is the feedforward network we use to solve the XOR example. It has a single hidden layer containing two units. *(Left)*In this style, we draw every unit as a node in the graph. This style is very explicit and unambiguous but for networks larger than this example it can consume too much space. *(Right)*In this style, we draw a node in the graph for each entire vector representing a layer's activations. This style is much more compact.

Figure: A simple feed-forward network (Goodfellow et al, 2017, Fig. 6.2)

In mathematical notation:

$$y_i = \mathbf{w}^T \underbrace{g(\mathbf{W}^T \mathbf{x}_i + \mathbf{b}_1)}_{\mathbf{h}} + \mathbf{b}_2$$

UPPSALA UNIVERSITET

The Feed-Forward Network

$$y_i = \mathbf{w}^T g(\mathbf{W}^T \mathbf{x}_i + \mathbf{b}_1) + \mathbf{b}_2$$

UPPSALA UNIVERSITET

The Feed-Forward Network

$$y_i = \mathbf{w}^T g(\mathbf{W}^T \mathbf{x}_i + \mathbf{b}_1) + \mathbf{b}_2$$

$$W = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, w = \begin{pmatrix} 1 \\ -2 \end{pmatrix}, b_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, b_2 = (0), x_i = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

UPPSALA UNIVERSITET

The Feed-Forward Network

$$y_i = \mathbf{w}^T g(\mathbf{W}^T \mathbf{x}_i + \mathbf{b}_1) + \mathbf{b}_2$$

$$W = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, w = \begin{pmatrix} 1 \\ -2 \end{pmatrix}, b_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, b_2 = (0), x_i = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

$$g(z) = \mathrm{ReLU}(z) = \max(0, z)$$

UPPSALA UNIVERSITET

The Feed-Forward Network

$$y_i = \mathbf{w}^T g(\mathbf{W}^T \mathbf{x}_i + \mathbf{b}_1) + \mathbf{b}_2$$

$$W = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, w = \begin{pmatrix} 1 \\ -2 \end{pmatrix}, b_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, b_2 = (0), x_i = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

$$g(z) = \mathrm{ReLU}(z) = \max(0, z)$$

$$y_i = \begin{pmatrix} 1 \\ -2 \end{pmatrix}^T \mathrm{ReLU}\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) + (0)$$

$$= \begin{pmatrix} 1 \\ -2 \end{pmatrix}^T \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (0) = 1$$

UPPSALA UNIVERSITET

The Feed-Forward Network

A feed-forward network for one observation (x_i).

$$\underbrace{\mathbf{h}_1}_{1\times k_1} = g_1(\underbrace{\mathbf{x}^T}_{1\times p}\underbrace{\mathbf{W}_1}_{p\times k_1} + \underbrace{\mathbf{b}_1}_{1\times k_1})$$

$$\vdots$$

$$\underbrace{\mathbf{h}_l}_{1\times k_l} = g_l(\underbrace{\mathbf{h}_{l-1}^T}_{1\times k_{l-1}}\underbrace{\mathbf{W}_l}_{k_{l-1}\times k_l} + \underbrace{\mathbf{b}_l}_{1\times k_l})$$

$$\vdots$$

$$\underbrace{\hat{\mathbf{y}}}_{1\times m} = g_L(\underbrace{\mathbf{h}_{L-1}^T}_{1\times k_{l-1}}\underbrace{\mathbf{W}_L}_{k_{l-1}\times m} + \underbrace{\mathbf{b}_L}_{1\times m})$$

$$\hat{y} = f_L(f_{L-1}(...f_1(x)...))$$

UPPSALA UNIVERSITET

Output units (g_L)

- Depend on the data y

UPPSALA UNIVERSITET

Output units (g_L)

- Depend on the data y
- Linear units for regression

$$\hat{y} = \mathbf{wh} + \mathbf{b}$$

UPPSALA UNIVERSITET

Output units (g_L)

- Depend on the data y
- Linear units for regression

$$\hat{y} = \mathbf{wh} + \mathbf{b}$$

- Bernoulli units for binary classification

$$\hat{y} = \sigma(\mathbf{wh} + \mathbf{b}),$$

where

$$\sigma(z) = \frac{1}{1 + \exp(-z)},$$

i.e. the logistic or sigmoid function.

UPPSALA UNIVERSITET

Output units (g_L)

- Multinoulli units for multi-class classification

$$\hat{\mathbf{y}} = \text{softmax}(\mathbf{wh} + \mathbf{b}) \,,$$

where

$$\text{softmax}(\mathbf{z})_i = \frac{\exp(z_i)}{\sum_j \exp(z_j)} \,.$$

UPPSALA UNIVERSITET

Output units (g_L)

- Multinoulli units for multi-class classification

$$\hat{\mathbf{y}} = \text{softmax}(\mathbf{wh} + \mathbf{b}),$$

where

$$\text{softmax}(\mathbf{z})_i = \frac{\exp(z_i)}{\sum_j \exp(z_j)}.$$

- Other situations: Use the negative log-likelihood, e.g. Poisson, ordinal logit, survival models

UPPSALA UNIVERSITET

Activation functions (g_l)

- Sometimes use notation σ as in $\sigma(Wh + b)$

UPPSALA UNIVERSITET

Activation functions (g_l)

- Sometimes use notation σ as in $\sigma(Wh + b)$
- Historically $g(z)$ has been the sigmoid or or hyperbolic tangent (tanh)

$$g_{\text{sigmoid}}(z) = \frac{e^z}{e^z + 1} = \frac{1}{1 + e^{-z}}$$

$$g_{\tanh}(z) = \frac{\sinh z}{\cosh z} = \frac{e^{2z} - 1}{e^{2z} + 1}$$

UPPSALA UNIVERSITET

Activation functions (g_l)

- Sometimes use notation σ as in $\sigma(Wh + b)$
- Historically $g(z)$ has been the sigmoid or or hyperbolic tangent (tanh)

$$g_{\text{sigmoid}}(z) = \frac{e^z}{e^z + 1} = \frac{1}{1 + e^{-z}}$$

$$g_{\tanh}(z) = \frac{\sinh z}{\cosh z} = \frac{e^{2z} - 1}{e^{2z} + 1}$$

- Today, variants of Rectified linear unit (ReLU) is common
  - Easier to estimate with SGD
  - Easier for deep models

UPPSALA UNIVERSITET

Activation functions (g_l): ReLU

$$g_{\text{ReLU}}(z) = \max(0, z)$$

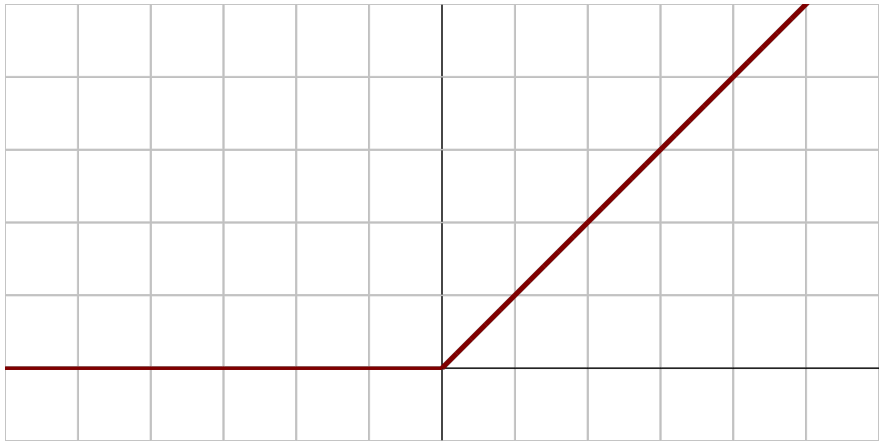


Figure: Rectified Linear Unit (Wikipedia)

UPPSALA UNIVERSITET

Activation functions (g_l): GeLU

$$g_{\text{GeLU}}(z) = z\Phi(z)$$

where $\Phi(z)$ is a standard Gaussian.

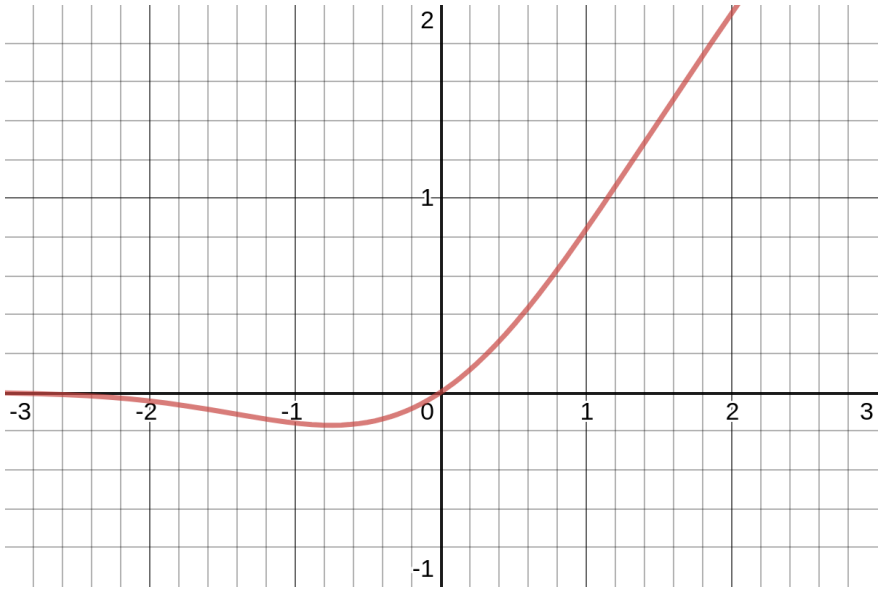


Figure: Gaussian Error Linear Unit (Wikipedia)

UPPSALA UNIVERSITET

Activation functions (g_l): ELU

$$g_{\text{ELU}}(z) = \begin{cases} \alpha\left(e^z - 1\right), & \text{if } z < 0, \\ z, & \text{if } z \geq 0. \end{cases}$$

where α is commonly set to 1.

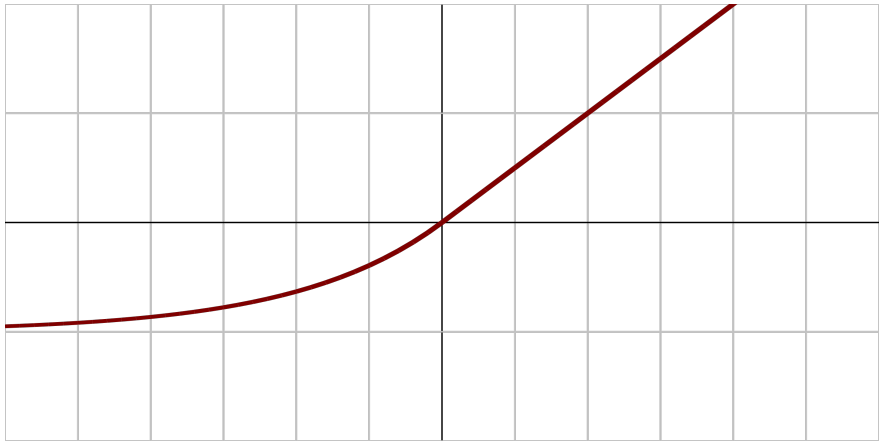


Figure: Exponential Linear Unit (Wikipedia)

UPPSALA UNIVERSITET

Architecture design

- Architecture: the overall structure of the network
- Choices:
  - How many layers?
  - How many hidden units in each layer?
  - Activation functions?

UPPSALA UNIVERSITET

Architecture design

- Architecture: the overall structure of the network
- Choices:
  - How many layers?
  - How many hidden units in each layer?
  - Activation functions?
- *Note!* Output units is defined by both the data and by design

UPPSALA UNIVERSITET

Universal Approximation Theorem

- A feed-forward neural network with one hidden layer and a non-polynomial activation (e.g., sigmoid, tanh, ReLU) can approximate any continuous function on a compact set $K \subset \mathbb{R}^n$.

UPPSALA UNIVERSITET

Universal Approximation Theorem

- A feed-forward neural network with one hidden layer and a non-polynomial activation (e.g., sigmoid, tanh, ReLU) can approximate any continuous function on a compact set $K \subset \mathbb{R}^n$.
- Formally, for any continuous function $f : K \to \mathbb{R}^m$ and any $\varepsilon > 0$, there exists a one-hidden-layer network

$$g(x) = C\,\sigma(Ax + b)$$

such that

$$\sup_{x \in K} \|f(x) - g(x)\| < \varepsilon.$$

UPPSALA UNIVERSITET

Universal Approximation Theorem

- A feed-forward neural network with one hidden layer and a non-polynomial activation (e.g., sigmoid, tanh, ReLU) can approximate any continuous function on a compact set $K \subset \mathbb{R}^n$.
- Formally, for any continuous function $f : K \to \mathbb{R}^m$ and any $\varepsilon > 0$, there exists a one-hidden-layer network

$$g(x) = C\,\sigma(Ax + b)$$

such that

$$\sup_{x \in K} \|f(x) - g(x)\| < \varepsilon.$$

- Interpretation: The worst-case error between the network g and the target function f on the entire set K can be made arbitrarily small by using enough hidden units.

UPPSALA UNIVERSITET

Universal Approximation Theorem, but...

- Neural networks are universal function approximators, but...

UPPSALA UNIVERSITET

Universal Approximation Theorem, but...

- Neural networks are universal function approximators, but...
  - No guarantee we can learn the network

UPPSALA UNIVERSITET

Universal Approximation Theorem, but...

- Neural networks are universal function approximators, but...
  - No guarantee we can learn the network
  - No guarantee that it will generalize

UPPSALA UNIVERSITET

Universal Approximation Theorem, but...

- Neural networks are universal function approximators, but...
  - No guarantee we can learn the network
  - No guarantee that it will generalize
  - No indication of how large the network needs to be

UPPSALA UNIVERSITET

Depth matters

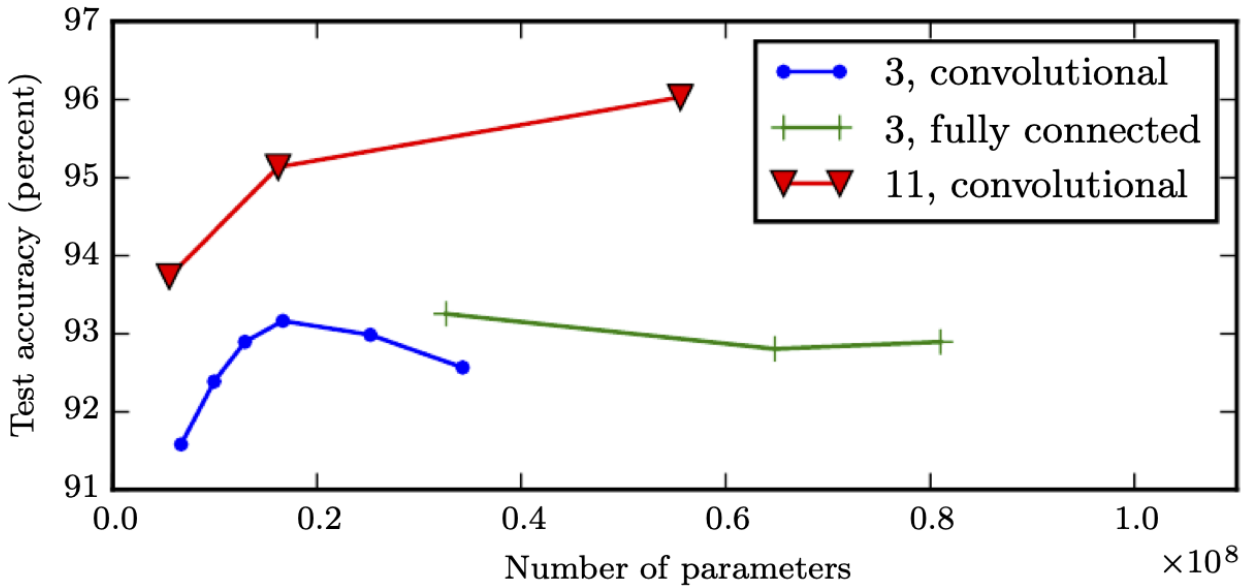


Figure: Effect of depth on accuracy (Goodfellow et al, 2017, Fig. 6.3)

UPPSALA UNIVERSITET

Depth matters II

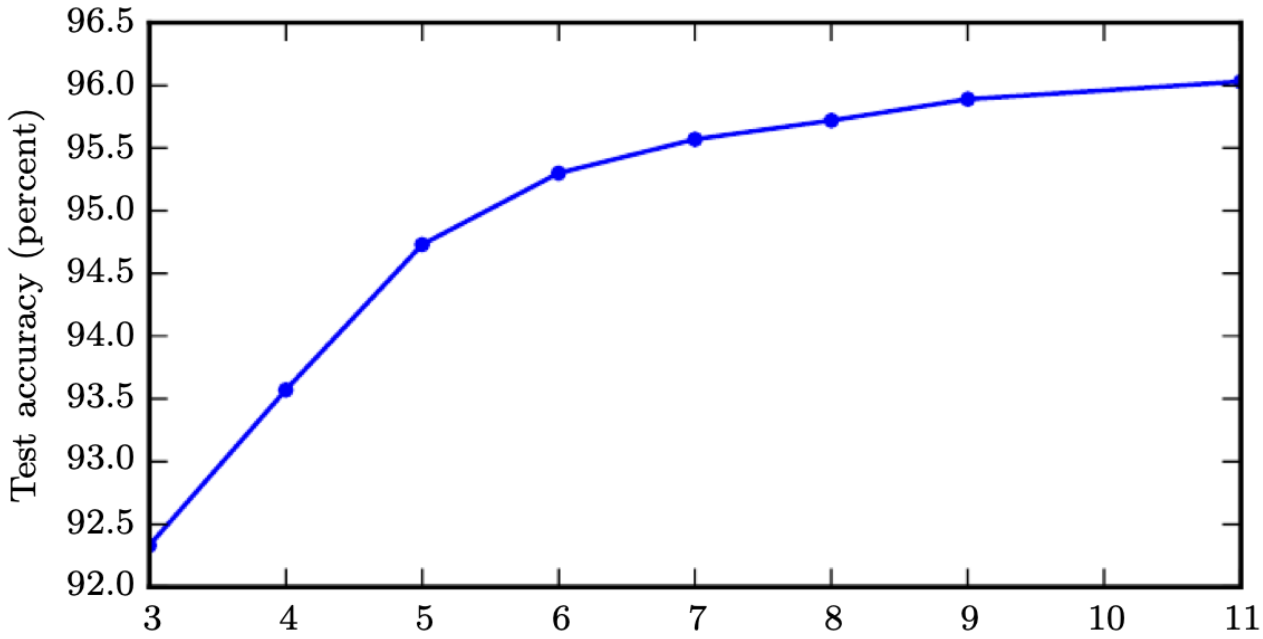


Figure: Depth vs. no of parameters (Goodfellow et al, 2017, Fig. 6.6)

UPPSALA UNIVERSITET

How to choose architecture

- Trial and error on validation sets
- Art rather than science, however...

UPPSALA UNIVERSITET

How to choose architecture

- Trial and error on validation sets
- Art rather than science, however...
  1. Start: get training error to zero

UPPSALA UNIVERSITET

How to choose architecture

- Trial and error on validation sets
- Art rather than science, however...
  1. Start: get training error to zero
  2. Regularize: get validation error to minimum
- Specialized approaches (Bayesian optimization)

UPPSALA UNIVERSITET

How to choose architecture

- Trial and error on validation sets
- Art rather than science, however...
  1. Start: get training error to zero
  2. Regularize: get validation error to minimum
- Specialized approaches (Bayesian optimization)
- Grid search (combinatorial explosion)
  - Really bad if many hyperparameters has a little effect
  - If we have 5 irrelevant parameters we try 3 values for: 125 training per relevant run
- Instead use...

UPPSALA UNIVERSITET

How to choose architecture

- Trial and error on validation sets
- Art rather than science, however...
  1. Start: get training error to zero
  2. Regularize: get validation error to minimum
- Specialized approaches (Bayesian optimization)
- Grid search (combinatorial explosion)
  - Really bad if many hyperparameters has a little effect
  - If we have 5 irrelevant parameters we try 3 values for: 125 training per relevant run
- Instead use...Random search

UPPSALA UNIVERSITET

Grid search vs. Random Search

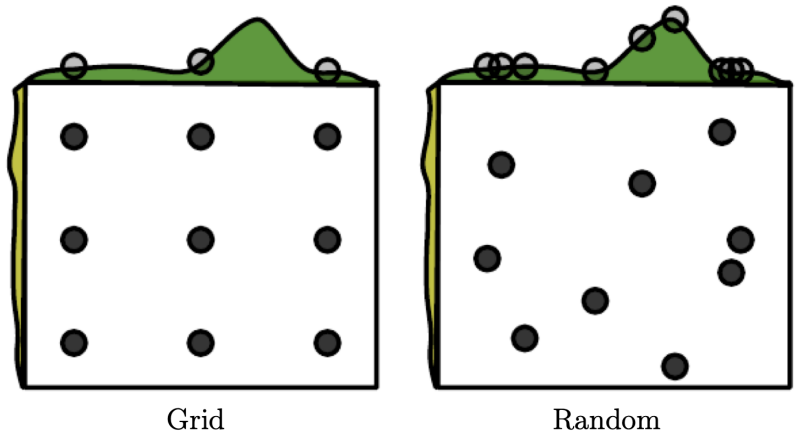


Figure: Grid search and random search (Goodfellow et al, 2017, Fig. 11.2)

UPPSALA UNIVERSITET

Section 3

Regularization

UPPSALA UNIVERSITET

Regularization of Neural Networks

- Reduce training error but improve generalization error

UPPSALA UNIVERSITET

Regularization of Neural Networks

- Reduce training error but improve generalization error
- Neural Networks are extremely flexible / high model capacity

UPPSALA UNIVERSITET

Regularization of Neural Networks

- Reduce training error but improve generalization error
- Neural Networks are extremely flexible / high model capacity
- Regularization is important for good generalizability

UPPSALA UNIVERSITET

Norm penalty

- Let

$$\tilde{J}(W, b) = J(W, b) + \alpha\Omega(W),$$

  where $J(W, b)$ is the cost function and $\alpha\Omega(W)$ is the penalty for the weight matrices.
- α is the strength of the penalty.

UPPSALA UNIVERSITET

Norm penalty

- Let

$$\Omega_1(W) = \sum_i \sum_j |w|_{i,j} ,$$

and

$$\Omega_2(W) = \sum_i \sum_j w_{i,j}^2 ,$$

be the L_1 and L_2 regularization respectively.

- We can then get the cost function

$$\tilde{J}(W, b) = J(W, b) + \sum_l \alpha_l \Omega_2(W_l) ,$$

UPPSALA UNIVERSITET

Weight decay

- Let's define the cost function as

$$\begin{aligned}\tilde{J}(w) &= J(w) + \alpha\Omega_2(w) \\ &= J(w) + \alpha w^T w\end{aligned}$$

- Then the gradient update becomes

$$\nabla_w \tilde{J}(w) = \nabla_w J(w) + 2\alpha w$$

- To update our weights with gradient descent

$$w \leftarrow w - \epsilon(\nabla_w J(w) + 2\alpha w)$$

UPPSALA UNIVERSITET

Weight decay

- Let's define the cost function as

$$\begin{aligned}\tilde{J}(w) &= J(w) + \alpha\Omega_2(w) \\ &= J(w) + \alpha w^T w\end{aligned}$$

- Then the gradient update becomes

$$\nabla_w \tilde{J}(w) = \nabla_w J(w) + 2\alpha w$$

- To update our weights with gradient descent

$$w \leftarrow w - \epsilon(\nabla_w J(w) + 2\alpha w)$$

$$w \leftarrow (1 - 2\alpha\epsilon)w - \epsilon\nabla_w J(w)$$

UPPSALA UNIVERSITET

Weight decay / Norm penalty

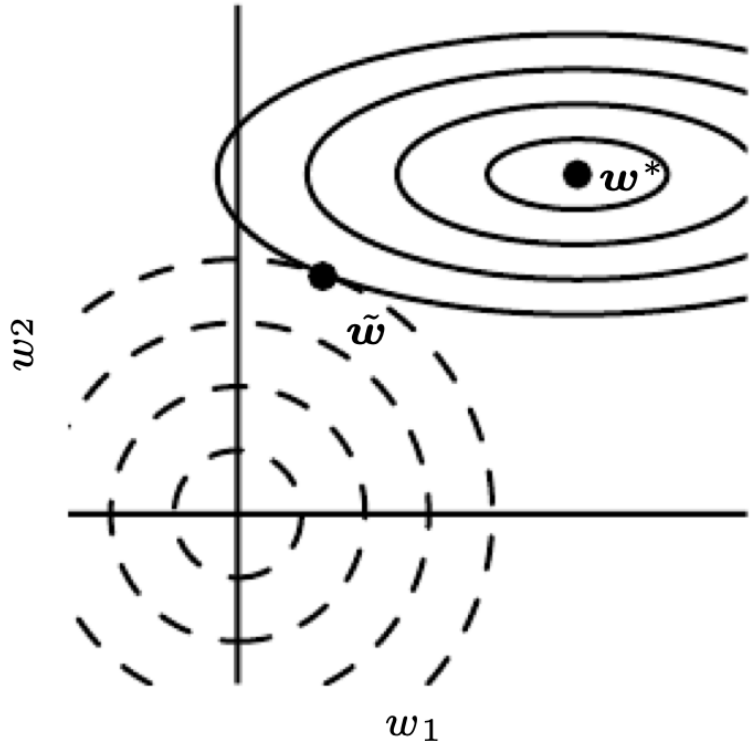


Figure: L_2 regularization (Goodfellow et al, 2017, Fig. 7.1)

UPPSALA UNIVERSITET

Dataset augmentation

Figure: Data Augmentation (Chollet and Allair, 2018, Fig 5.10)

- "Modify" data or inject noise
- Common in Convolutional neural networks

UPPSALA UNIVERSITET

Multi-Task Learning

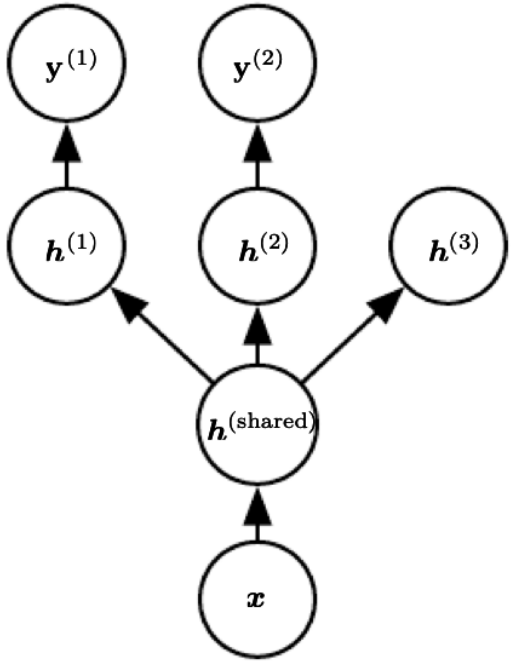


Figure: Multi-task learning (Goodfellow et al., 2017, Fig 7.2)

- Common in Pre-Trained Language Models (Transformers)

UPPSALA UNIVERSITET

Early Stopping

- Stop optimization early based on validation error

UPPSALA UNIVERSITET

Early Stopping

- Stop optimization early based on validation error
- Use the best iteration (hyperparameter)

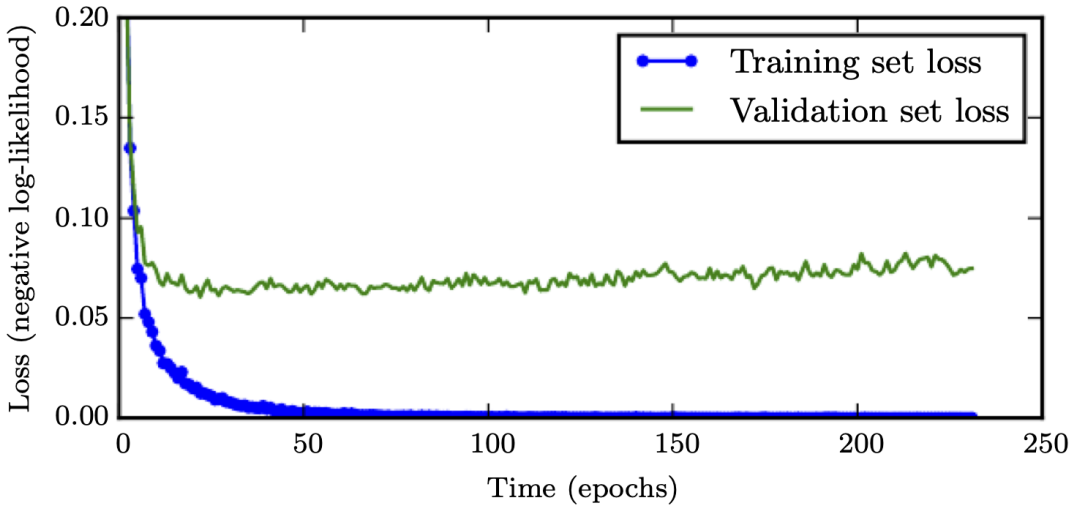


Figure: Early Stopping (Goodfellow et al, 2017, Fig. 7.3)

- Can be shown to be equivalent (under strict assumptions) to L_2 regularization (see Goodfellow et al, 2017)
- Efficient regularization

UPPSALA UNIVERSITET

Early Stopping

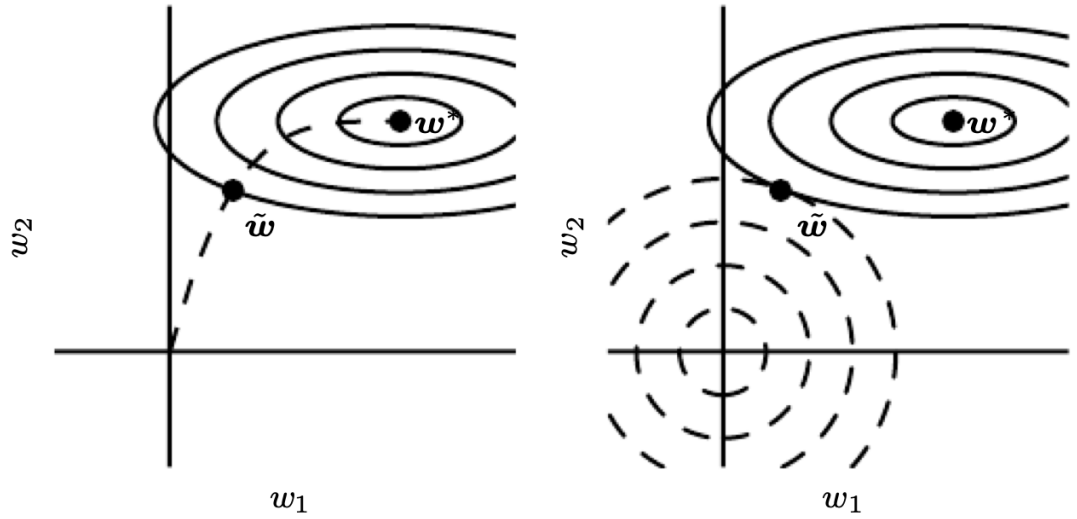


Figure: Early Stopping (Goodfellow et al, 2017, Fig. 7.4)

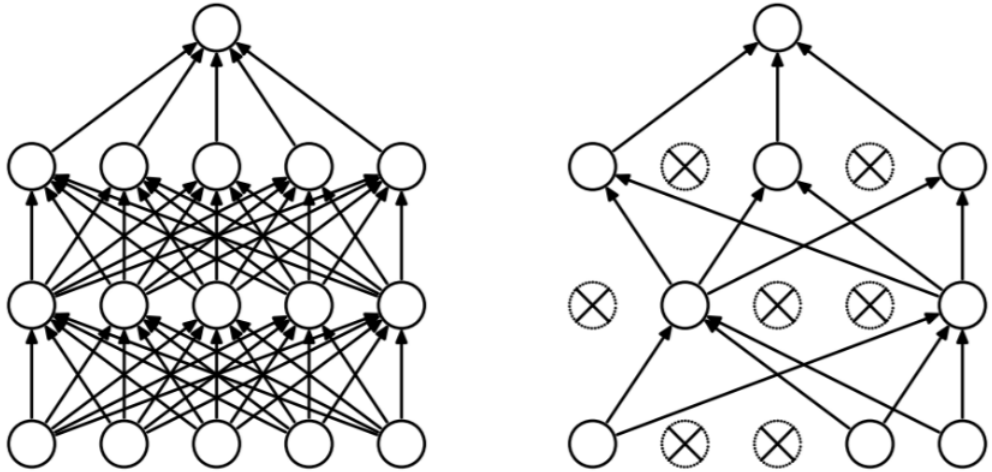
UPPSALA UNIVERSITET

Dropout

- In each iteration:
  - Sample an indicator I_i for each node i
  - Set the value h_i to 0 with probability p
- The dropout probability (dropout rate) is typically 0.2 for input nodes and 0.5 for hidden nodes
- Forces the network to
  - not rely on individual nodes
  - spread out the weights over more nodes
- Can be seen as an ensemble method

UPPSALA UNIVERSITET

Dropout



(a) Standard Neural Net (b) After applying dropout.

Figure 1: Dropout Neural Net Model. **Left**: A standard neural net with 2 hidden layers. **Right**: An example of a thinned net produced by applying dropout to the network on the left. Crossed units have been dropped.

Figure: Dropout (Srivastava et al, 2014)

UPPSALA UNIVERSITET

But...

The best regularizer is...

UPPSALA UNIVERSITET

But...

The best regularizer is... to get more data.

UPPSALA UNIVERSITET

Section 4

Optimization of Neural Networks

UPPSALA UNIVERSITET

Neural Network Learning

- Usually, a lot of data and many parameters ($\theta = (W, b)$)

UPPSALA UNIVERSITET

Neural Network Learning

- Usually, a lot of data and many parameters ($\theta = (W, b)$)
- We usually minimize our training cost function

$$J(\theta) = \sum_{i}^{N} L(\mathrm{NN}(x_i|\theta), y_i) + \Omega(\theta)\,,$$

where L is the observation level loss, NN() is our neural network and Ω is the regularization term.

UPPSALA UNIVERSITET

Neural Network Learning

- Usually, a lot of data and many parameters ($\theta = (W, b)$)
- We usually minimize our training cost function

$$J(\theta) = \sum_{i}^{N} L(\mathrm{NN}(x_i|\theta), y_i) + \Omega(\theta)\,,$$

  where L is the observation level loss, NN() is our neural network and Ω is the regularization term.
- Learning Target: Find $\hat{\theta}$ that minimize the generalization error

UPPSALA UNIVERSITET

Optimization of Neural Networks

- Stochastic Gradient Descent methods

$$\theta_t = \theta_{t-1} - \eta_t \hat{\nabla} J(\theta_{t-1}),$$

where η_t denotes the learning rate at iteration t and $\hat{\nabla} J(\theta_{t-1})$ is an estimate of the gradient of the objective function.

UPPSALA UNIVERSITET

Optimization of Neural Networks

- Stochastic Gradient Descent methods

$$\theta_t = \theta_{t-1} - \eta_t \hat{\nabla} J(\theta_{t-1}),$$

  where η_t denotes the learning rate at iteration t and $\hat{\nabla} J(\theta_{t-1})$ is an estimate of the gradient of the objective function.
- In practice, better optimizers are used:
  - Adam (the main optimizer today)
  - RMSprop

UPPSALA UNIVERSITET

Optimization of Neural Networks

- Stochastic Gradient Descent methods

$$\theta_t = \theta_{t-1} - \eta_t \hat{\nabla} J(\theta_{t-1}),$$

  where η_t denotes the learning rate at iteration t and $\hat{\nabla} J(\theta_{t-1})$ is an estimate of the gradient of the objective function.
- In practice, better optimizers are used:
  - Adam (the main optimizer today)
  - RMSprop
- To compute $\hat{\nabla} J(\theta_{t-1})$:
  - Backpropagation algorithm (chain-rule for derivatives)

UPPSALA UNIVERSITET

Backpropagation

- Backpropagation provides an efficient procedure for computing all parameter gradients $\nabla J(\theta)$ in a feed-forward neural network.
- Uses the chain rule to propagate the error backward through layers:

$$\frac{\partial J}{\partial W_l} = h_{l-1}^\top \delta_l, \qquad \frac{\partial J}{\partial b_l} = \delta_l,$$

  where δ_l is the error signal at layer l.
- The algorithm consists of two passes:
  - **Forward pass:** compute

$$h_l = g_l(h_{l-1}^\top W_l + b_l)$$

    for each layer l.
  - **Backward pass:** compute error signals

$$\delta_l = \left(\delta_{l+1} W_{l+1}^\top\right) \odot g_l'(z_l), \qquad z_l = h_{l-1}^\top W_l + b_l,$$

    starting from the output layer.

UPPSALA UNIVERSITET

Backpropagation

- Backpropagation provides an efficient procedure for computing all parameter gradients $\nabla J(\theta)$ in a feed-forward neural network.
- Uses the chain rule to propagate the error backward through layers:

$$\frac{\partial J}{\partial W_l} = h_{l-1}^\top \delta_l, \qquad \frac{\partial J}{\partial b_l} = \delta_l,$$

  where δ_l is the error signal at layer l.
- The algorithm consists of two passes:
  - **Forward pass:** compute

$$h_l = g_l(h_{l-1}^\top W_l + b_l)$$

    for each layer l.
  - **Backward pass:** compute error signals

$$\delta_l = \left(\delta_{l+1} W_{l+1}^\top\right) \odot g_l'(z_l), \qquad z_l = h_{l-1}^\top W_l + b_l,$$

    starting from the output layer.
- Enables efficient gradient-based optimization even for networks with many layers and millions of parameters.

UPPSALA UNIVERSITET

Forward Pass: Simple Example

- Consider a network with one hidden layer (2 units, we skip biases for simplicity) and ReLU activation:

$$h_1 = g_1(x^\top W_1), \qquad \hat{y} = w^\top h_1.$$

- Let

$$x = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad W_1 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}, \qquad w = \begin{bmatrix} 1 \\ -2 \end{bmatrix}.$$

- Compute hidden pre-activation:

$$z_1 = x^\top W_1 = \begin{bmatrix} -1 \\ 4 \end{bmatrix}.$$

- Apply ReLU:

$$h_1 = g_{\text{ReLU}}(z_1) = \max(0, z_1) = \begin{bmatrix} 0 \\ 4 \end{bmatrix}.$$

- Output:

$$\hat{y} = w^\top h_1 = -8.$$

UPPSALA UNIVERSITET

Backward Pass: Simple Example

- Loss (squared error):

$$J = \tfrac{1}{2}(\hat{y} - y)^2, \qquad y = 0, \qquad \frac{\partial J}{\partial \hat{y}} = \hat{y} - y = -8.$$

- Output layer gradients:

$$\frac{\partial J}{\partial w} = \frac{\partial J}{\partial \hat{y}} \cdot \frac{\partial \hat{y}}{\partial w} = h_1(\hat{y} - y) = \begin{bmatrix} 0 \\ -40 \end{bmatrix}.$$

- Backpropagated error signal:

$$\delta_1 := \frac{\partial J}{\partial z_1} = \frac{\partial J}{\partial \hat{y}} \cdot \frac{\partial \hat{y}}{\partial h_1} \cdot \frac{\partial h_1}{\partial z_1} = (\hat{y} - y)\, w \odot g'_{\mathsf{ReLU}}(z_1).$$

$$(\hat{y} - y)\, w = \begin{bmatrix} -8 \\ 16 \end{bmatrix}, \qquad g'_{\mathsf{ReLU}}(z_1) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad \delta_1 = \begin{bmatrix} 0 \\ 16 \end{bmatrix}.$$

- Gradients for first layer:

$$\frac{\partial J}{\partial W_1} = \frac{\partial J}{\partial \hat{y}} \cdot \frac{\partial \hat{y}}{\partial h_1} \cdot \frac{\partial h_1}{\partial z_1} \cdot \frac{\partial z_1}{\partial W_1} = x\, \delta_1^\top = \begin{bmatrix} 0 & 16 \\ 0 & 32 \end{bmatrix}.$$

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?
- A problem if local optima has a high cost/bad performance

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?
- A problem if local optima has a high cost/bad performance
- Good thing: This is probably not the situation!

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?
- A problem if local optima has a high cost/bad performance
- Good thing: This is probably not the situation!
- Many practitioners believe this is a problem

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?
- A problem if local optima has a high cost/bad performance
- Good thing: This is probably not the situation!
- Many practitioners believe this is a problem
- Diagnosis: Plot the gradient norm, $\mathbf{g}^T\mathbf{g}$, where $\mathbf{g} = \hat{\nabla} J(\theta)$

UPPSALA UNIVERSITET

Problems: Local Minima

- Neural Networks cost function $J(\theta)$ are (usually) not a convex function
- We can have local minima
- When will this be a problem?
- A problem if local optima has a high cost/bad performance
- Good thing: This is probably not the situation!
- Many practitioners believe this is a problem
- Diagnosis: Plot the gradient norm, $\mathbf{g}^T\mathbf{g}$, where $\mathbf{g} = \hat{\nabla} J(\theta)$

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- Another problem is saddle points

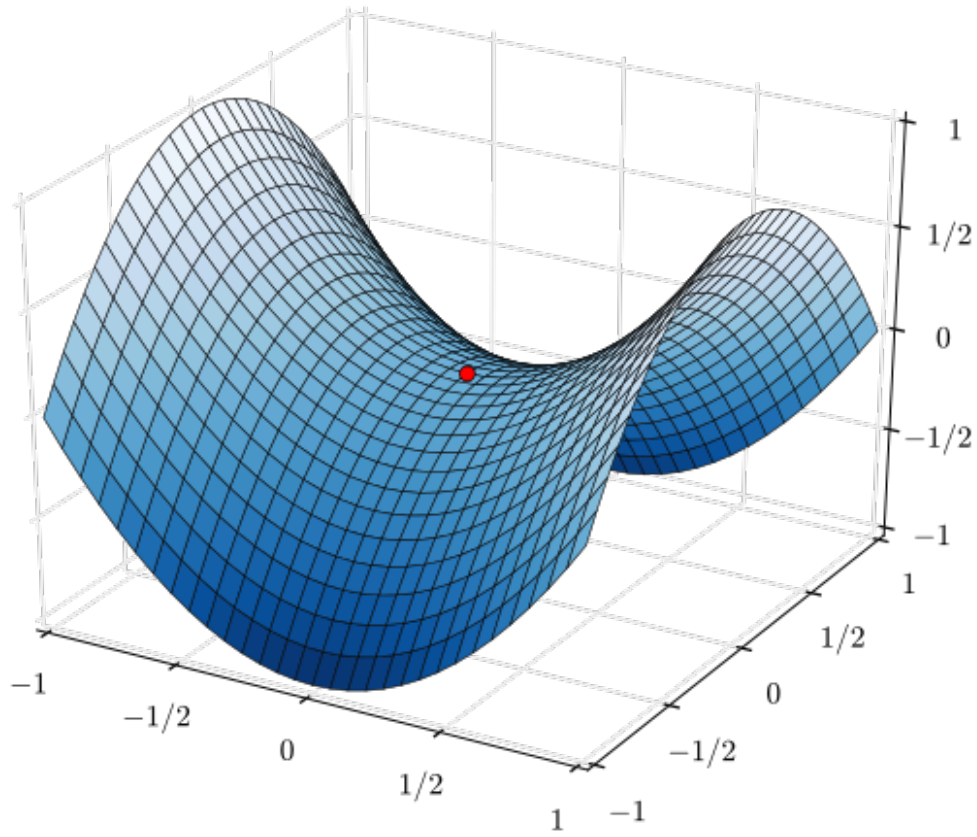


Figure: Saddle point for $z = x^2 - y^2$ (Wikipedia)

- What is the gradient in a saddle point?

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- In a saddle point the Hessian is indefinite, both positive and negative eigenvalues

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- In a saddle point the Hessian is indefinite, both positive and negative eigenvalues
- A local minimum: Hessian is positive definite, only positive eigen values

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- In a saddle point the Hessian is indefinite, both positive and negative eigenvalues
- A local minimum: Hessian is positive definite, only positive eigen values
- In random functions of high dimension: most points are saddle points
- Intuition: In random functions the sign of the eigen values of the Hessian is random

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- In a saddle point the Hessian is indefinite, both positive and negative eigenvalues
- A local minimum: Hessian is positive definite, only positive eigen values
- In random functions of high dimension: most points are saddle points
- Intuition: In random functions the sign of the eigen values of the Hessian is random
- In random functions: eigen values become more positive in regions of lower cost. I.e. local minima more probable in low cost regions. Saddle points more common in high-cost regions

UPPSALA UNIVERSITET

Problems: Plateaus and Saddle Points

- In a saddle point the Hessian is indefinite, both positive and negative eigenvalues
- A local minimum: Hessian is positive definite, only positive eigen values
- In random functions of high dimension: most points are saddle points
- Intuition: In random functions the sign of the eigen values of the Hessian is random
- In random functions: eigen values become more positive in regions of lower cost. I.e. local minima more probable in low cost regions. Saddle points more common in high-cost regions
- The problem of saddle points:
  - Probably a reason why second order methods (using the Hessian) has not succeed
  - Empirically, (stochastic) gradient descent seem to escape saddle points

UPPSALA UNIVERSITET

Problems: Cliffs

- Another problem is "cliffs" or large changes in gradients

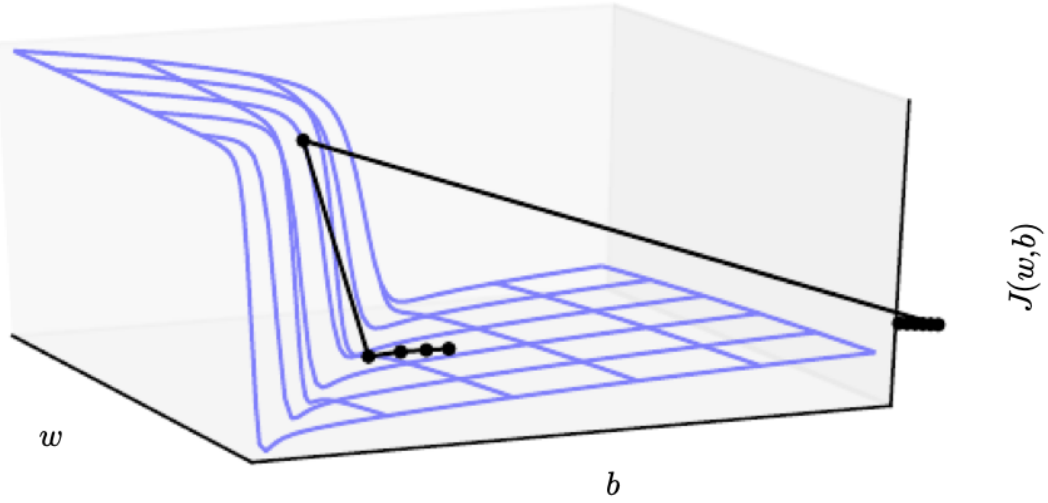


Figure: Cliff (Goodfellow et al., 2017, Fig. 8.3)

- Can undo many iterative steps
- Common in Recurrent neural networks
- Mitigation: Gradient clipping

UPPSALA UNIVERSITET

Problems: Explodig and vanishing gradients

- In deep neural networks, gradients can vanish or explode
- As an example: We want to compute the gradient for a situation where the weights are multiplied t times. Then using eigendecomposition

$$W^t = V \text{diag}(\lambda)^t V^T$$

- The gradient is scaled wrt $\text{diag}(\lambda)^t$

UPPSALA UNIVERSITET

Problems: Explodig and vanishing gradients

- In deep neural networks, gradients can vanish or explode
- As an example: We want to compute the gradient for a situation where the weights are multiplied t times. Then using eigendecomposition

$$W^t = V \text{diag}(\lambda)^t V^T$$

- The gradient is scaled wrt $\text{diag}(\lambda)^t$
- Cliffs is an example of gradient explosion
- Mitigation for graident explosion: Gradient clipping

UPPSALA UNIVERSITET

Problems: Explodig and vanishing gradients

- In deep neural networks, gradients can vanish or explode
- As an example: We want to compute the gradient for a situation where the weights are multiplied t times. Then using eigendecomposition

$$W^t = V \text{diag}(\lambda)^t V^T$$

- The gradient is scaled wrt $\text{diag}(\lambda)^t$
- Cliffs is an example of gradient explosion
- Mitigation for graident explosion: Gradient clipping
- Common problem in Recurrent neural networks

UPPSALA UNIVERSITET

Initial values

- We need to have starting values for gradient descent

UPPSALA UNIVERSITET

Initial values

- We need to have starting values for gradient descent
- Initialization can be seen as a hyperparameter

UPPSALA UNIVERSITET

Initial values

- We need to have starting values for gradient descent
- Initialization can be seen as a hyperparameter
- Bad initial values might
  - Bad convergence (local optimum)
  - Numerical problems

UPPSALA UNIVERSITET

Initial values

- We need to have starting values for gradient descent
- Initialization can be seen as a hyperparameter
- Bad initial values might
  - Bad convergence (local optimum)
  - Numerical problems
- We want to break symmetry between layers
  - Otherwise the same units will be updated in the same way (deterministically)

UPPSALA UNIVERSITET

Initial values

- We need to have starting values for gradient descent
- Initialization can be seen as a hyperparameter
- Bad initial values might
  - Bad convergence (local optimum)
  - Numerical problems
- We want to break symmetry between layers
  - Otherwise the same units will be updated in the same way (deterministically)
- Good practice
  - Initialize values randomly close to zero (uniform or normal)

UPPSALA UNIVERSITET

Section 5

Neural Networks in Practice

UPPSALA UNIVERSITET

TensorFlow

- Framework for large-scale machine learning and Neural Networks
- Developed by Google
- Can be used both from R and Python
- Used in both research and production
- What Tesorflow does:
  - Computing gradients (autodiff) for Neural Networks
  - Enable use of graphical processing units (GPU) and Tensor processing Units (TPU)
  - Enable training using common optimizers (such as Adam, RMSprop)
- Tesorflow Probability is a probabilistic programming framework using TF

UPPSALA UNIVERSITET

(Py)Torch

- Similar to TensorFlow
- Developed by Meta AI
- Can be used both from R and Python
- Used in both research and production
- pyro is a probabilistic programming framework using torch

UPPSALA UNIVERSITET

Keras

- Syntax for 'building' Neural Networks
- Available both in R and Python
- TensorFlow or Torch as backend