REPETITION LECTURE

INF5860 — Machine Learning for Image Analysis

Ole-Johan Skrede 05.06.2018

University of Oslo

- $\cdot\,$ Dense neural networks
- · CNN architectures
- $\cdot\,$ Object detection and image segmentation
- · Unsupervised learning
- · Generative adversarial networks

DENSE NEURAL NETWORKS

 $\cdot\,$ Given a training set with input x and desired output y

$$\Omega_{\text{train}} = \{ (x^{(1)}, y^{(1)}), \dots, (x^{(m)}, y^{(m)}) \}$$

 $\cdot\,$ Create a function f that "approximates" this mapping

 $f(x) \approx y, \quad \forall (x,y) \in \Omega_{\text{train}}$

 \cdot Hope that this generalises well to unseen examples, such that

$$f(x) = \hat{y} \approx y, \quad \forall (x, y) \in \Omega_{\text{test}}$$

where $\Omega_{\rm test}$ is a set of relevant unseen examples.

 \cdot Hope that this is also true for all unseen relevant examples.

DEEP LEARNING

- 1. Build a function f that maps input to output
 - · Input: Array of numbers.
 - $\cdot\,$ Output: Probability mass function conditional on observed input.
- 2. This function will have multiple layers, where each layer is a representation of the previous.
- 3. Measure how well the output of the function is approximating the true output
- 4. Use information from the error to update the function
- 5. Repeat step 3 and 4 with multiple training examples



ALL CONNECTIONS



5

ACTIVATION IN NODE 3 OF LAYER 1



6

ACTIVATION IN NODE 4 OF LAYER 2



7

- Functions that introduce non-linearity to our network
- Without it, our network just becomes a linear mapping from input to output
- Enables DNN to become *universal function approximators*
- $\cdot\,$ Can in theory be any function that is
 - \cdot Non-linear
 - Differentiable (if you are using a gradient-based optimization)







(c) Rectified linear unit (ReLU)

$$z_k^{[L]} = \sum_{j=1}^{n^{[L-1]}} w_{jk}^{[L]} a_j^{[L-1]} + b_k^{[L]}$$
$$a_k^{[L]} = s(z_k^{[L]})$$
$$= \hat{y}_k$$

for

$$k = 1, \dots, n_y,$$

= 1, \dots, n^{[L]}.



$$s(z)_k = \frac{e^{z_k}}{\sum_{i=1}^n e^{z_i}}$$

- $\cdot \sum_k s(z)_k = 1$, and the softmax can be interpreted as a probability
- Using the softmax as our final activation, we can interpret the output of our network as

$$f(x;\theta)_k = \Pr(Y = k | X = x; \theta) \quad (1)$$

- X is a random vector modeling our input
- Y is a categorical random variable modeling the true output
- $\cdot \, \, \theta$ is the collection of parameters

$$\theta = \{ w_{jk}^{[l]}, b_k^{[l]} \}$$

for

$$\begin{cases} j &= 1, \dots, n^{[l-1]} \\ k &= 1, \dots, n^{[l]} \\ l &= 1, \dots, L \end{cases}$$

• The neural network is set up, the next step is to determine the values of the parameters

$$\theta = \{ w_{jk}^{[l]}, b_k^{[l]} : j \in \left\{ 1, \dots, n^{[l-1]} \}, k \in \{1, \dots, n^{[l]} \}, l \in \{1, \dots, L\} \right\}$$

- This is done by defining a cost function which is to be minimized by some optimization method.
- In the most common case, we minimize the *cross entropy* cost function using a *stochastic gradient descent* optimizer

CROSS ENTROPY COST FUNCTION

- \cdot We can derive the cross entropy cost function from maximum likelihood
- \cdot The maximum likelihood estimator (MLE) $\hat{\theta}$ of θ is the parameter

$$\hat{\theta} = \arg\max_{\theta} \ell(\theta; x) \tag{2}$$

- The *likelihood* $\ell(\theta; x)$ is our network $p_Y(y|X = x; \theta)$, when x is a fixed realization of X, and θ is a variable.
- We then showed in the lecture that the maximum likelihood estimator is found by minimizing

$$J(\theta, \Omega_{\text{train}}) = -\frac{1}{m} \sum_{i=1}^{m} \sum_{k=1}^{n_y} \tilde{y}_k^{(i)} \log \hat{y}_k^{(i)}.$$
(3)

- $\cdot \hat{y}$ is the network output vector, \tilde{y} is the one-hot encoded reference. m is the number of training examples, and n_y is the number of classes.
- \cdot In practice, we approximate this by minimizing over a mini-batch $\Omega^{mb}_{
 m train} \subset \Omega_{
 m train}$

GRADIENT DESCENT

$$\theta \leftarrow \theta - \lambda \nabla_{\theta} J(\theta) \tag{4}$$

• The gradient of J w.r.t. a set of variables $\theta = [\theta_1, \dots, \theta_m]$

$$\nabla_{\theta}J = \left[\frac{\partial J}{\partial \theta_1}, \dots, \frac{\partial J}{\partial \theta_m}\right]$$

- $\cdot \nabla_{\theta} J(\theta_k)$ gives the direction of steepest ascent at the point θ_k
- $\cdot \ \lambda$ determines how long to move in that direction



 $\cdot\,$ We need to compute the values of

$$rac{\partial J}{\partial w_{jk}^{[l]}}$$
 and $rac{\partial J}{\partial b_k^{[l]}}$.

for all nodes and edges in the network.

- $\cdot\,$ This is doen by the so-called backprop algorithm
- It works by successive use of the chain rule, from the last layer backward to the first



$$\frac{\partial J}{\partial w_{jk}^{[l]}} = \frac{\partial J}{\partial z_k^{[l]}} a_j^{[l-1]}, \quad l = 1, \dots, L.$$
(5a)

$$\frac{\partial J}{\partial b_k^{[l]}} = \frac{\partial J}{\partial z_k^{[l]}}, \quad l = 1, \dots, L.$$
(5b)

$$\frac{\partial J}{\partial z_k^{[l]}} = g'(z_k^{[l]}) \sum_{j=1}^{n^{[l+1]}} \frac{\partial J}{\partial z_j^{[l+1]}} w_{kj}^{[l+1]}, \quad l = 1, \dots, L-1$$
(5c)
$$\frac{\partial J}{\partial z_k^{[L]}} = \hat{y}_k - \tilde{y}_k.$$
(5d)

Note that

- \cdot Eqs. (5a)— (5c) are generally applicable
- · Eq. (5d) assumes that J is the cross-entropy loss, and that $a^{[L]} = s(z^{[L]})$ with s as the softmax function.
- $\cdot\,$ We also have vectorized versions of these equations

CNN ARCHITECTURES

- A well-performing image classification network from 2014
- $\cdot\,$ Simple and elegant design
 - $\cdot \;$ alternating $2 \times 2 \; \text{maxpool}$
 - $\cdot \;$ multiple 3×3 convolution layers
- Expencive, both in terms of memory and computation
 - $\cdot\,$ Very many parameters
 - \cdot Many layers (at the time)
 - · "Unsophisticated" architecture



ResNet's motivational problem

- · Deeper models seems to be better
- · However, very deep models perform worse
- · Not due to overtraining
- · Degradation problem





- \cdot A deeper model should not have higher training error
- \cdot "Proof" by construction
 - $\cdot\,$ Take a shallow model
 - · Insert extra layers as identity mappings
 - $\cdot\,$ This deeper mode should have at least as good training error
- $\cdot\,$ How to solve this is the key

- · Stack a couple of layers
- $\cdot \operatorname{Input} x$
- $\cdot \, \operatorname{Let} H(x)$ be the desired mapping to be learned



- · Explicitly compose the output as H(x) = F(x) + x, by adding the input x
- $\cdot\,$ This means that what has been learnt is the residual F(x)=H(x)-x
- · This should make identities H(x) = xeasier to learn
- $\cdot\,$ Easier to train very deep networks





Figure 2: Left: a regular residual block. Right: a "bottleneck" residual block



OBJECT DETECTION AND IMAGE SEGMENTATION

IMAGE CLASSIFICATION AND OBJECT LOCALIZATION

- $\cdot\,$ Classify an image with a single object
- · Draw a bounding box around the object



Figure 3: Seagull. Image source: https://www.pixabay.com

TARGET VECTOR

- \cdot Add object/no object indicator c_0
- · Interpret c_0 as $c_0 = \Pr(\text{there is an object in this box})$
- c₀ is often referred to as the *objectness*, but can also be thought of as a "catch-all" background class indicator
- · Standard category probabilities from classification $(c_1, c_2, \ldots, c_{N_c})$
- · Interpret c_i as $c_i = \Pr(\text{class}_i | c_0 = 1)$, $i = 1, \dots, N_c$
- $\cdot\,$ Add bounding box location specifiers
 - $\cdot \ b_r$: Center row coordinate
 - $\cdot \ b_c$: Center column coordinate
 - $\cdot b_h$: Box height
 - $\cdot b_w$: Box width



EXAMPLE: BIG CATS

 $\cdot c_1$: Tiger

- \cdot c_2 : Leopard
- \cdot c_3 : Lion





EXAMPLE: BIG CATS

 $\cdot c_1$: Tiger

 \cdot c_2 : Leopard

 \cdot c_3 : Lion





EXAMPLE: BIG CATS

- $\cdot c_1$: Tiger
- \cdot c_2 : Leopard
- \cdot c_3 : Lion

 $\hat{y} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ b_r \\ b_c \\ b_h \\ b_w \end{bmatrix}$

Note that $c_0 = 0$, so we do not care about the rest, symbolized by ϕ .



MULTI-TASK LOSS FUNCTION

 \cdot Partition y into y = [c, b], with

$$\cdot \ c = [c_0, c_1, \dots, c_{N_c}]$$

$$b = [b_r, b_c, b_h, b_w]$$

 $\cdot \ L_2$ loss for object bounding box location b

$$L_b(\hat{b}, b) = \sum_{i \in \{x, y, h, w\}} (\hat{b}_i - b_i)^2$$

 \cdot Cross entropy loss for object categories c

$$L_c(\hat{c}, c) = -\sum_{i=1}^n c_i \log \hat{c}_i$$

 $\cdot\,$ The total loss can be written as

$$L(\hat{y}, y) = L_c + [c_0 > 0]L_b$$

 $\cdot\,$ Only compare bounding box if there is an object in the image

• Proportion of positive reference instances labeled as positive by the proposed method

$$tpr = \frac{|B_R \cap B_P|}{|B_R|}$$

- $\cdot\,$ Also known as
 - *true positive rate* (tpr)
 - recall
- Example on the right is pixel classification, but it also applies to object instances



Figure 8: Top: reference (green), proposal (blue). Middle: True positive (red). Bottom: Reference positive (red). Image source: https://www.pixabay.com

• Proportion of negative reference instances labeled as negative by the proposed method

$$nr = \frac{\left| (B_R \cup B_P)^c \right|}{|B_R^c|}$$

· Also known as true negative rate (tnr)



Figure 9: Top: reference (green), proposal (blue). Middle: True negative (red). Bottom: Reference negative (red). Image source: https://www.pixabay.com

• Proportion of proposed positive instances that are also labeled positive by the reference

$$ppv = \frac{|B_R \cap B_P|}{|B_P|}$$

- · Also known as *positive predictive value* (ppv)
- Example on the right is pixel classification, but it also applies to object instances



Figure 10: Top: reference (green), proposal (blue). Middle: True positive (red). Bottom: Proposed positive (red). Image source: https://www.pixabay.com

 The proportion of all instances classified as positive by the reference and/or the proposal method, that are classified as positive by both the reference and the proposal method

$$iou = \frac{|B_R \cap B_P|}{|B_R \cup B_P|}$$

- $\cdot\,$ Also known as
 - · Intersection over Union (IoU)
 - · Tanimoto index
- Example on the right is pixel classification, but it also applies to object instances



Figure 11: Top: reference (green), proposal (blue). Middle: Intersection (red). Bottom: Union (red). Image source: https://www.pixabay.com

• Get region proposals (as in R-CNN)



- \cdot Get region proposals (as in R-CNN)
- $\cdot\,$ Run a CNN on the entire image



- \cdot Get region proposals (as in R-CNN)
- $\cdot\,$ Run a CNN on the entire image
- Project region proposals (ROIs) onto output CNN feature map



- \cdot Get region proposals (as in R-CNN)
- $\cdot\,$ Run a CNN on the entire image
- Project region proposals (ROIs) onto output CNN feature map
- · ROI pooling layer



- \cdot Get region proposals (as in R-CNN)
- $\cdot\,$ Run a CNN on the entire image
- Project region proposals (ROIs) onto output CNN feature map
- · ROI pooling layer
- Feed the fixed-sized pooled region to fully connected layers
- $\cdot\,$ One softmax output for class prediction
- $\cdot\,$ One regression output for the bounding box prediction



- \cdot Get region proposals (as in R-CNN)
- $\cdot\,$ Run a CNN on the entire image
- Project region proposals (ROIs) onto output CNN feature map
- · ROI pooling layer
- Feed the fixed-sized pooled region to fully connected layers
- $\cdot\,$ One softmax output for class prediction
- $\cdot\,$ One regression output for the bounding box prediction
- · Multi-task loss







- $\cdot\,$ Segment image all at once
- $\cdot \,$ Input image shape: $H \times W \times C$
- $\cdot \;$ Output layer shape: $H \times W \times N_{c}$, where N_{c} : number of classes
- Pixel-wise cross entropy loss
 - $\cdot\,$ Softmax over channels at a pixel location
 - $\cdot\,$ Repeat, and average over all pixels
- $\cdot\,$ Very expensive on computation and memory



Figure 12: Top: Original. Bottom: Segmented. Image source: https://www.pexels.com

- · Segment image all at once
- $\cdot \,$ Input image shape: $H \times W \times C$
- $\cdot \;$ Output layer shape: $H \times W \times N_c$, where N_c : number of classes
- Spatial downsampling followed by upsampling (encoding, decoding)
- $\cdot\,$ Pixel-wise cross entropy loss
 - $\cdot\,$ Softmax over channels at a pixel location
 - $\cdot\,$ Repeat, and average over all pixels
- · Different upsampling techniques



Figure 13: Top: Original. Bottom: Segmented. Image source: https://www.pexels.com

MAX UNPOOLING

Remember max locations from max pool downsampling. Reverse this on the "opposite" layer





INTERPOLATION UPSAMPLING



- Can view convolution as a matrix-matrix multiplication
- Transposed convolution gets its name by transposing this operation
- $\cdot\,$ Also called
 - \cdot fractionally strided convolution
 - · econvolution (this is a misnomer)



- Insert spacing between convolution kernel cells (dilation rate)
- \cdot Also called
 - $\cdot\,$ convolution with holes
 - A-trous convolution (a trous is french for with holes)



UNSUPERVISED LEARNING

T-DISTRIBUTED STOCHASTIC NEIGHBOUR EMBEDDING (T-SNE)

- · Transforms high-dimensional (hd) data points to low-dimensional (ld) data ponts
- $\cdot\,$ Aims to preserve neighbourhood identity between data points
- \cdot Similar (close) hd points should also be similar (close) in the ld representation
- \cdot For each point *i*, we define two distributions:
 - $\cdot p_i(x_i,x_j)$: The probability that x_i and x_j are "neighbours",
 - $\cdot \ q_i(y_i,y_j)$: The probability that y_i and y_j are "neighbours",
- $\cdot \, p_i$ are distributions over all hd neighbours x
- $\cdot \, q_i$ are distributions over all ld neighbours y
- $\cdot\,$ For p, we use symmetric gaussian distributions
- $\cdot \,$ For q , we use symmetric student-t distributions
- $\cdot\,$ We make q similar to p by minimizing the KL-divergence between the two
- \cdot The KL-divergence is minimized by determining the ld points y with gradient descent

AUTOENCODERS

- $\cdot\,$ An autoencoder f consist of an encoder g and an decoder h
- \cdot The encoder maps the input x to some representation z

$$g(x) = z$$

- \cdot We often call this representation z for the code or the latent vector
- \cdot The decoder maps this representation z to some output \hat{x}

$$g(z) = \hat{x}$$

 $\cdot\,$ We want to train the encoder and decoder such that

 $f(x) = h(g(x)) = \hat{x} \approx x$

• Commonly used for compression, feature extraction and de-noising



COMPRESSION AUTOENCODER - MNIST EXAMPLE





DE-NOISING AUTOENCODER — MNIST EXAMPLE





- A variational autoencoder is designed to have a continuous latent space
- This makes them ideal for random sampling and interpolation
- $\cdot\,$ It achieve this by forcing the encoder g to generate Gaussian representations, $z\sim\mathcal{N}(\mu,\sigma^2)$
- $\cdot\,$ More precisely, for one input, the encoder generates a mean μ and a variance σ^2
- \cdot We sample then sample a zero-mean, unit-variance Gaussian $\tilde{z}\sim\mathcal{N}(0,1)$
- $\cdot\,$ Construct the input z to the decoder from this

$$z = \mu + \tilde{z}\sigma^2$$

 \cdot With this, z is sampled from $q = \mathcal{N}(\mu, \sigma^2)$



INTUITION

- $\cdot\,$ This is a stochastic sampling
- $\cdot \,$ That is, we can sample different z from the same set of (μ,σ^2)
- The intuition is that the decoder "learns" that for a given input x:
 - \cdot the point z is important for reconstruction
 - $\cdot\,$ but also a neighbourhood of z
- In this way, we have smoothed the latent space, at least locally
- $\cdot\,$ In the previous lecture, we learnt ways to achieve this

- \cdot We can guide the solutions by restricting the generative distribution q
- $\cdot\,$ We do this by making it approximate some distribution p
- \cdot In that way, the latent vectors, even for different categories, will be relatively close
- \cdot The desired distribution used in variational autoencoders is the standard normal $p=\mathcal{N}(0,1)$
- We use the familiar KL-divergence between the desired and the generated distribution as a regularizer in the loss function
- \cdot With this, the total loss for an example x_i is something like

$$J(x_i) = ||x^{(i)} - f(x^{(i)})|| + D_{KL}(p||q_{\mu_i,\sigma_i})$$

- $\cdot\,$ That is, the sum what we call the *reconstruction loss* and the *latent loss*
- \cdot The latent loss for a single variable x_i can be shown to be equal to

$$D_{KL}(p||q_{\mu_i,\sigma_i}) = \frac{1}{2}(\mu_i^2 + \sigma_i^2 - \log \sigma_i^2 - 1)$$



VAE EXAMPLE: GENERATION OF NEW SIGNALS

- \cdot Sample a random latent vector z from $\mathcal{N}(0,1)$
- \cdot Decode z



- \cdot We generate a signal c that is an interpolation between two signals a and b
- \cdot We can do this by a linear interpolation between the means

$$\mu_{c_k} = (1 - w_k)\mu_a + w_k\mu_b$$

where the different interpolation weights can be

$$w_k = \frac{k}{n+1}, \quad k = 1, \dots, n$$



GENERATIVE ADVERSARIAL NETWORKS

COMPONENTS

- $\cdot\,$ A generator function that tries to create real-looking examples
- · A discriminator function that tries to distinguish real from fake examples
- · Functions are updated in a feedback loop, making each better at its task



 \cdot The discriminator is a function

 $D: x \mapsto D(x; \theta_D)$

mapping input x to $D(x; \theta_D)$ with parameters θ_D

 \cdot The generator is a function

 $G: z \mapsto G(z; \theta_G)$

mapping input z to $G(z; \theta_G)$ with parameters θ_G

- · The discriminator has an associated loss $J_D(\theta_D, \theta_G)$, depending on both θ_D and θ_G , but can only control θ_D
- · The generator has an associated loss $J_G(\theta_D, \theta_G)$, depending on both θ_D and θ_G , but can only control θ_G
- \cdot The optimal solution $(heta_D^*, heta_G^*)$ is a Nash equilibrium where
 - \cdot θ_D^* is a local minimum of J_D w.r.t. $heta_D$
 - $\cdot \hspace{0.1 cm} heta_{G}^{*}$ is a local minimum of J_{G} w.r.t. $heta_{G}$

THE GENERATOR

- $\cdot\,$ The generator is a differentiable function
- \cdot The input z is a random vector sampled from some simple prior distribution p_g
- \cdot The output x = G(z) is then sampled from p_m
- $\cdot\,$ The most common form of G is some kind of generative neural network
- \cdot If we have GAN trained on data from p_d , we can use the generator to sample from p_m
- $\cdot p_m \approx p_d$
- \cdot With this, samples from the generator will look like the training data



THE DISCRIMINATOR

- \cdot The discriminator is a standard classification network
- \cdot Trained to differentiate between real and fake (generated) images
- \cdot Outputs a single number in [0,1]
 - $\cdot D(x) = 0 \rightarrow D$ believes x is fake
 - $\cdot D(x) = 1 \rightarrow D$ believes x is real



- $\cdot\,$ At each update step, one mini-batch x of real images, and one mini-batch z of latent vectors are drawn
- $\cdot \, \, z$ is fed through ${\it G}$, producing ${\it G}(z)$
- $\cdot \ D(x)$ is compared with D(G(z))
- $\cdot \,\, heta_G$ is updated using gradients from J_G
- $\cdot \,\, heta_D$ is updated using gradients from J_D
- The discriminator and generator are updated in tandem using some regular optimization routine (SGD, Adam, etc.)
- \cdot Some flexibility with regards to updating one more often than the other



- The generator, *G*, and discriminator, *D*, are two distinct networks with distinct cost functions
- $\cdot\,$ The cost functions are optimized separately
- · The discriminator cost function is given by

$$J_D(\theta_D, \theta_G) = -E_{x \sim p_d} [\log D(x; \theta_D)] - E_{z \sim p_g} [\log(1 - D(G(z; \theta_G); \theta_D))]$$
$$= -E_{x \sim p_d} [\log D(x; \theta_D)] - E_{x \sim p_m} [\log(1 - D(x; \theta_D))]$$

 \cdot With discrete samples, over one mini-batch $\{x_i\}$ and $\{z_i\}$, this becomes

$$J_D(\theta_D, \theta_G) = -\frac{1}{m} \sum_{i=1}^{m} \left[\log(D(x_i; \theta_D)) + \log(1 - D(G(z_i; \theta_G); \theta_D)) \right]$$

- \cdot Binary classification with sigmoid cross entropy where
 - · Real images are given label 0
 - $\cdot\,$ Generated (fake) images are given label 1

 $\cdot\,$ For the generator cost, we propose the following

$$J_G(\theta_D, \theta_G) = -E_{z \sim p_g} \log D(G(z; \theta_G); \theta_D)$$
$$= -\frac{1}{m} \sum_{i=1}^m \log D(G(z_i; \theta_G); \theta_D)$$

- With this, the generator maximizes the log-probability of the discriminator being mistaken (assigning label 1 to the generated examples)
- Contrast this with the previous minimax game where we the generator minimizes the log-probability of the discriminator being correct (assigning label 0 to the generated examples)
- Both the generator and the discriminator now have strong gradients when they are "losing the game"

 $\cdot\,$ Minimizing the discriminative cost

$$J_D(\theta_D, \theta_G) = -\frac{1}{m} \sum_{i=1}^m \left[\log(D(x_i; \theta_D)) + \log(1 - D(G(z_i; \theta_G); \theta_D)) \right]$$

"pushes" D(x) to 1 (real class) and D(G(z)) to 0 (fake class)

· Minimizing the generative cost

$$J_G(\theta_D, \theta_G) = -\frac{1}{m} \sum_{i=1}^m \log(D(G(z_i; \theta_G); \theta_D))$$

"pushes" D(G(z)) to 1 (real class)



QUESTIONS?