

From Autoencoder to Variational Autoencoder

Hao Dong

Peking University



From Autoencoder to Variational Autoencoder

- Vanilla Autoencoder (AE)
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



From Autoencoder to Variational Autoencoder

Feature Representation

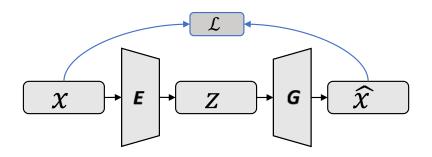
- Vanilla Autoencoder (AE)
- Denoising Autoencoder
- Sparse Autoencoder
- **Contractive Autoencoder**
- Stacked Autoencoder
- Distribution Representation
- Variational Autoencoder (VAE)



- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



What is it?



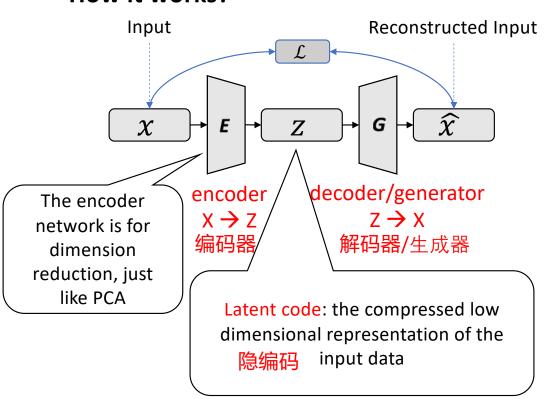
Reconstruct high-dimensional data using a neural network model with a narrow bottleneck layer.

The bottleneck layer captures the compressed latent coding, so the nice by-product is dimension reduction.

The low-dimensional representation can be used as the representation of the data in various applications, e.g., image retrieval, data compression ...



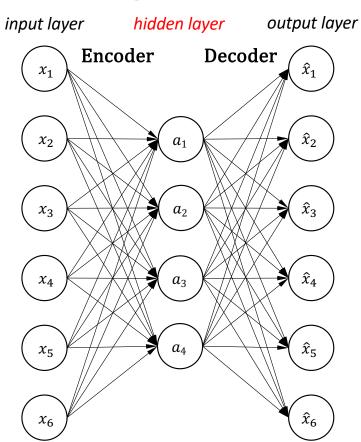
How it works?



Ideally the input and reconstruction are identical



Training



- The hidden units are usually less than the number of inputs
- Dimension reduction --- Representation learning

The distance between two data can be measure by Mean Squared Error (MSE):

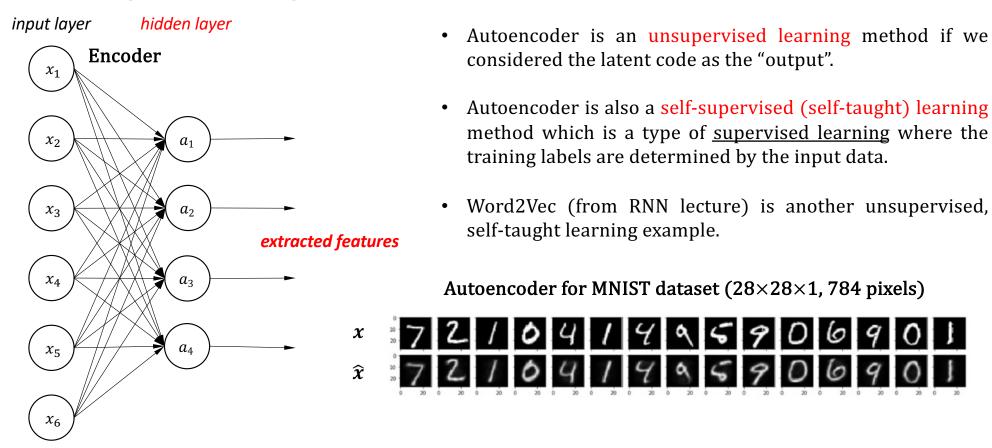
$$\mathcal{L} = \frac{1}{n} \sum_{i=1}^{n} (x^i - G(E(x^i)))^2$$

where n is the number of variables

• It is trying to learn an approximation to the identity function so that the input is "compress" to the "compressed" features, discovering interesting structure about the data.



Testing/Inferencing

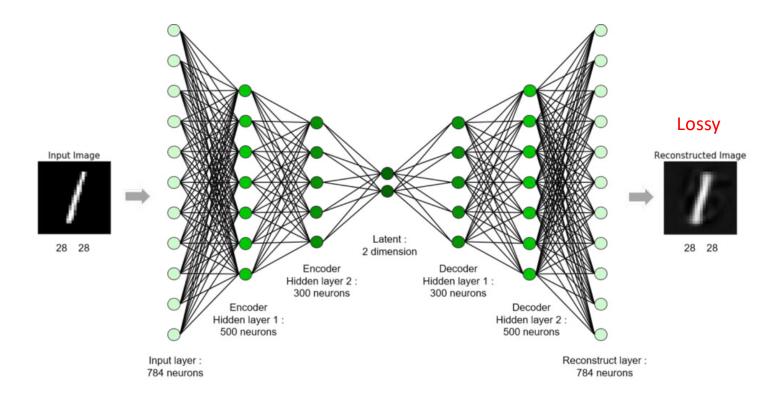


社主大学 PEKING UNIVERSITY

Vanilla Autoencoder

• Example:

• Compress MNIST (28x28x1) to the latent code with only 2 variables

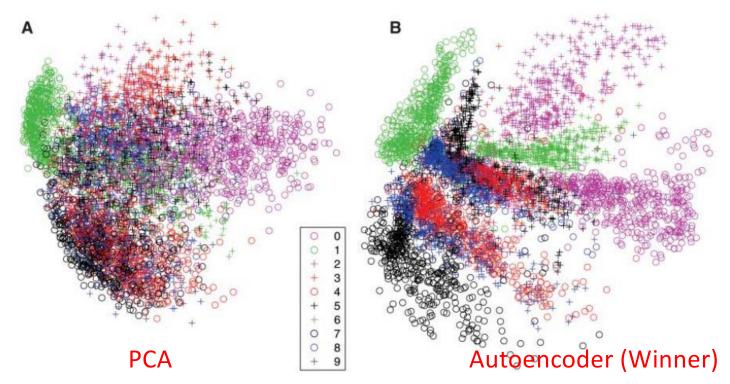






- Power of Latent Representation
 - t-SNE visualisation on MNIST: PCA vs. Autoencoder

Fig. 3. (A) The two-dimensional codes for 500 digits of each class produced by taking the first two principal components of all 60,000 training images. (B) The two-dimensional codes found by a 784-1000-500-250-2 autoencoder. For an alternative visualization, see (8).





Discussion

• Hidden layer is overcomplete if greater than the input layer



Discussion

- Hidden layer is overcomplete if greater than the input layer
 - No compression
 - No guarantee that the hidden units extract meaningful feature



- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



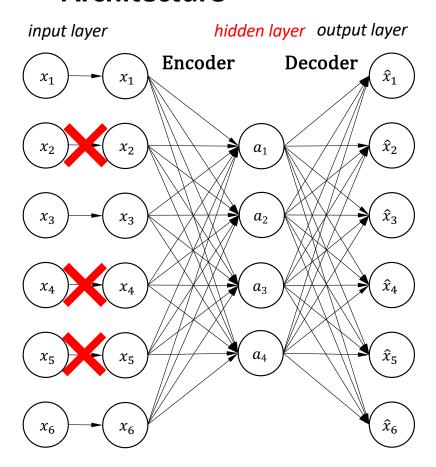


- Why?
 - Avoid overfitting
 - Learn robust representations



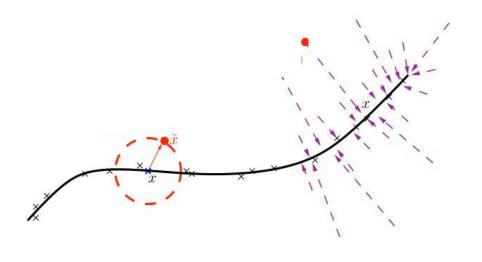
Denoising Autoencoder

Architecture



Applying dropout between the input and the first hidden layer

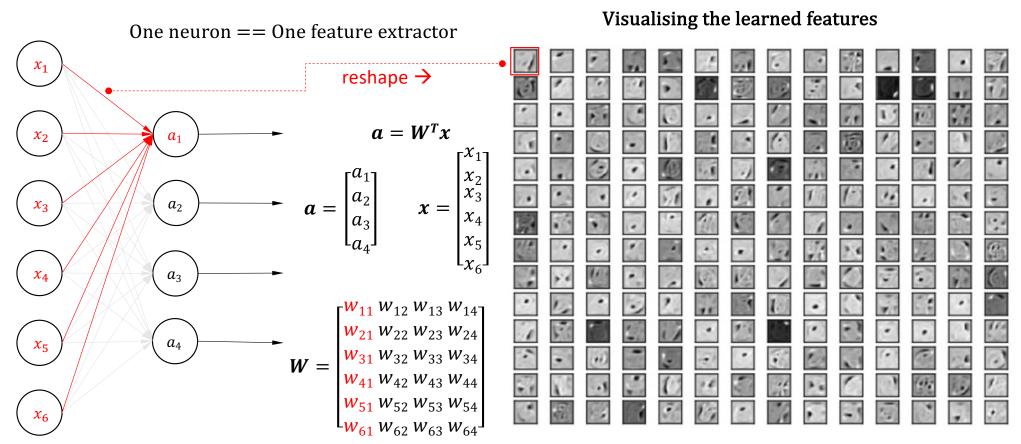
• Improve the robustness





Denoising Autoencoder

Feature Visualisation





Denoising Autoencoder

Denoising Autoencoder & Dropout

Denoising autoencoder was proposed in 2008, 4 years before the dropout paper (Hinton, et al. 2012).

Denoising autoencoder can be seem as applying dropout between the input and the first layer.

Denoising autoencoder can be seem as one type of data augmentation on the input.

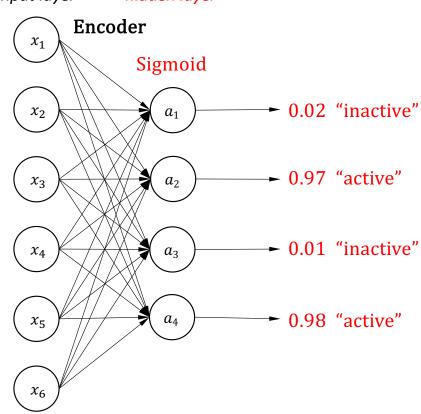


- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



• Why?





- Even when the number of hidden units is large (perhaps even greater than the number of input pixels), we can still discover interesting structure, by imposing other constraints on the network.
- In particular, if we impose a "sparsity" constraint on the hidden units, then the autoencoder will still discover interesting structure in the data, even if the number of hidden units is large.



Recap: KL Divergence

$$KL\Big(p(x)ig\|q(x)\Big) = \int p(x) \lnrac{p(x)}{q(x)} dx = \mathbb{E}_{x\sim p(x)}\left[\lnrac{p(x)}{q(x)}
ight]$$

Smaller == Closer

$$KL\Big(p(x)\Big\|q(x)\Big)=0\Leftrightarrow p(x)=q(x)$$

$$KL\Big(p(x)\Big\|q(x)\Big)=0\Leftrightarrow p(x)=q(x)$$

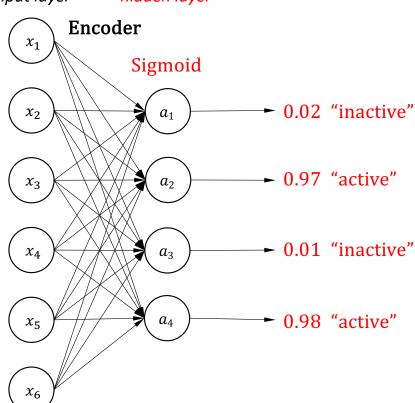
$$D_B\Bigl(p(x),q(x)\Bigr) = -\ln\int\sqrt{p(x)q(x)}dx$$

和京大学 PEKING UNIVERSITY

Sparse Autoencoder

Sparsity Regularisation

input layer hidden layer



Given M data samples (batch size) and Sigmoid activation function, the active ratio of an input a_i :

$$\hat{\rho}_j = \frac{1}{M} \sum_{m=1}^M a_j$$

To make the output "sparse", we would like to enforce the following constraint, where ρ is a "sparsity parameter", such as 0.2 (20% of the neurons)

$$\hat{\rho}_j = \rho$$

The penalty term is as follow, where \boldsymbol{s} is the number of activation outputs.

$$\mathcal{L}_{\rho} = \sum_{j=1}^{s} KL(\rho||\hat{\rho}_{j})$$

$$= \sum_{j=1}^{s} (\rho \log \frac{\rho}{\hat{\rho}_{j}} + (1-\rho) \log \frac{1-\rho}{1-\hat{\rho}_{j}})$$

The total loss:

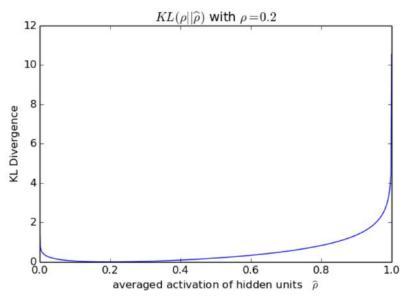
$$\mathcal{L}_{total} = \mathcal{L}_{MSE} + \lambda \mathcal{L}_{\rho}$$

The number of hidden units can be greater than the number of input variables.

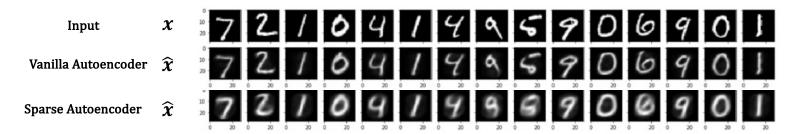


Sparsity Regularisation

Smaller $\rho ==$ More sparse



Autoencoders for MNIST dataset





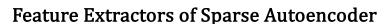
• Different regularisation loss

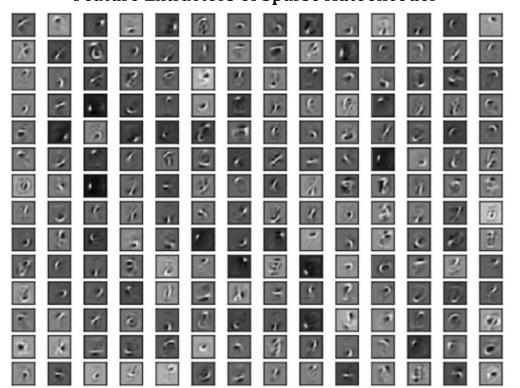
Method	Hidden Activation	Reconstruction Activation	Loss Function
Method 1	Sigmoid	Sigmoid	$\mathcal{L}_{total} = \mathcal{L}_{MSE} + \mathcal{L}_{\rho}$
Method 2	ReLU	Softplus	$\mathcal{L}_{total} = \mathcal{L}_{MSE} + \ \boldsymbol{a}\ $

 $\mathcal{L}_{\,1}$ on the hidden activation output

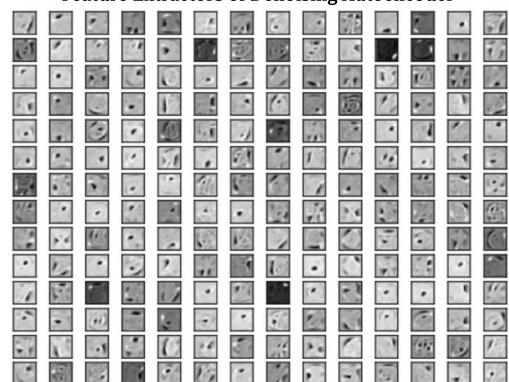


Sparse Autoencoder vs. Denoising Autoencoder





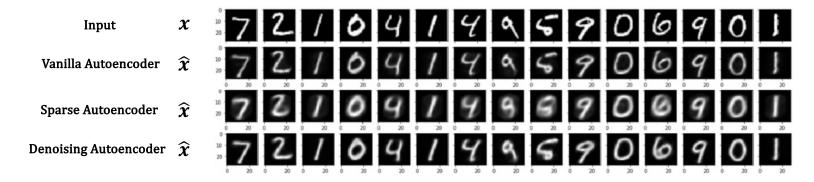
Feature Extractors of Denoising Autoencoder





Autoencoder vs. Denoising Autoencoder vs. Sparse Autoencoder

Autoencoders for MNIST dataset





- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



Why?

- Denoising Autoencoder and Sparse Autoencoder overcome the overcomplete problem via the input and hidden layers.
- Could we add an explicit term in the loss to avoid uninteresting features?

We wish the features that ONLY reflect variations observed in the training set



How

- Penalise the representation being too sensitive to the input
- Improve the robustness to small perturbations
- Measure the sensitivity by the Frobenius norm of the Jacobian matrix of the encoder activations



Recap: Jacobian Matrix

$$z = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \qquad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} z_1 + z_2 \\ 2z_1 \end{bmatrix} = f \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

$$x = f(z) \qquad z = f^{-1}(x) \qquad \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} x_2/2 \\ x_1 - x_2/2 \end{bmatrix} = f^{-1} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$J_f = \begin{bmatrix} \frac{\partial x_1}{\partial x_2} & \frac{\partial x_1}{\partial x_2} & \frac{\partial x_1}{\partial x_2} \\ \frac{\partial x_2}{\partial x_1} & \frac{\partial x_2}{\partial x_2} & \frac{\partial x_2}{\partial x_2} \end{bmatrix} \text{ output } \qquad J_f = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$$

$$J_{f^{-1}} = \begin{bmatrix} \frac{\partial z_1}{\partial x_1} & \frac{\partial z_1}{\partial x_2} & \frac{\partial z_1}{\partial x_2} \\ \frac{\partial z_2}{\partial x_1} & \frac{\partial z_2}{\partial x_2} & \frac{\partial z_1}{\partial x_2} \end{bmatrix} \qquad J_{f^{-1}} = I$$

$$\frac{29}{2}$$



Jacobian Matrix

$$y = \begin{bmatrix} f_1(x) \\ f_2(x) \\ f_3(x) \\ \vdots \\ f_n(x) \end{bmatrix}$$

$$y = \begin{bmatrix} f_1(x) \\ f_3(x) \\ \vdots \\ f_n(x) \end{bmatrix}$$

$$y = \begin{bmatrix} f_1(x) \\ f_2(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{bmatrix}$$

$$J(x_1, x_2, x_3, \dots x_n) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \frac{\partial f_1}{\partial x_3} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \frac{\partial f_2}{\partial x_3} & \dots & \frac{\partial f_2}{\partial x_n} \\ \frac{\partial f_3}{\partial x_1} & \frac{\partial f_3}{\partial x_2} & \frac{\partial f_3}{\partial x_3} & \dots & \frac{\partial f_3}{\partial x_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \frac{\partial f_n}{\partial x_3} & \dots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

$$y(x) \approx y(p) + J \bullet (x - p)$$



New Loss

$$\|J_f(x)\|_F^2 = \sum_{ij} (rac{\partial h_j(x)}{\partial x_i})^2$$

$$\mathcal{J}_{CAE}(heta) = \sum_{x \in D_n} (L(x, g(f(x))) + \lambda \|J_f(x)\|_F^2)$$

reconstruction

new regularisation



- vs. Denoising Autoencoder
 - Advantages
 - CAE can better model the distribution of raw data

- Disadvantages
 - DAE is easier to implement

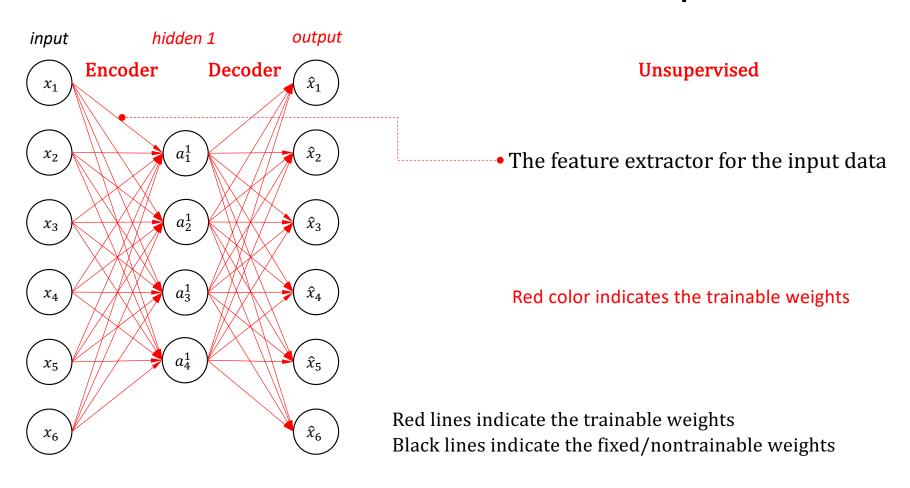


- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)



Stacked Autoencoder

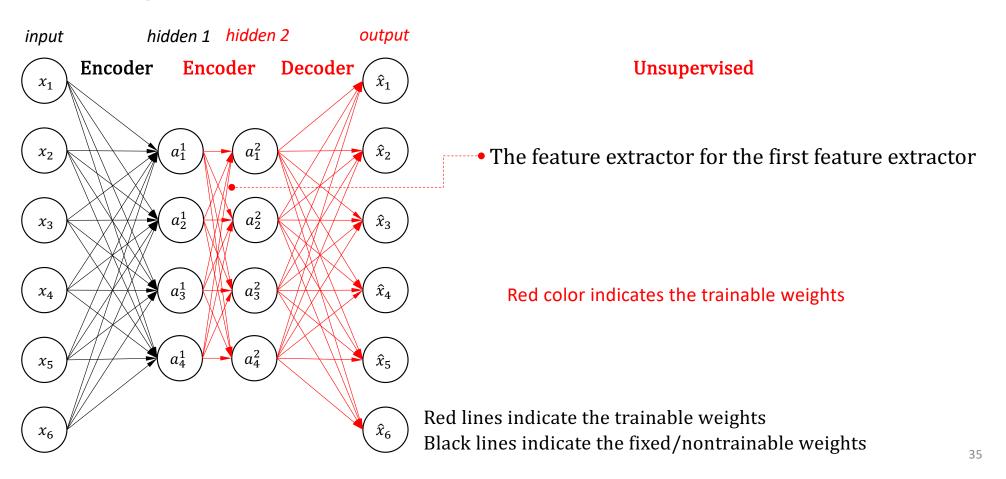
Start from Autoencoder: Learn Feature From Input





Stacked Autoencoder

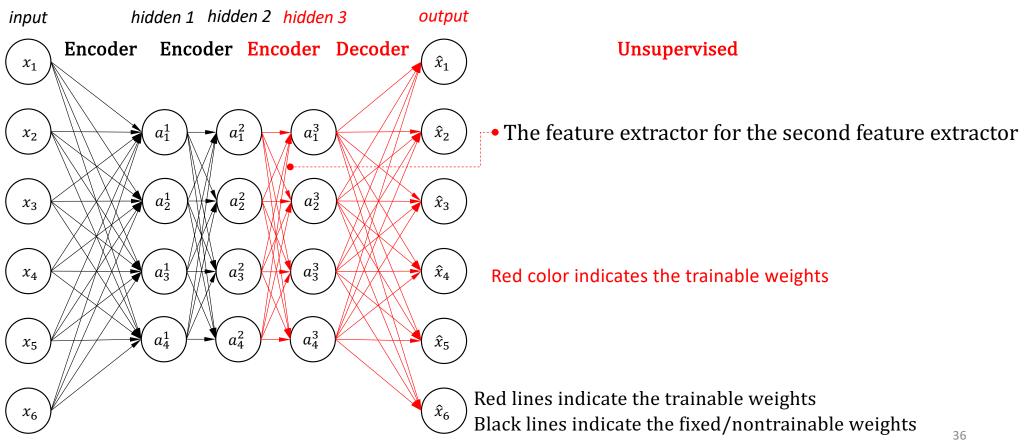
2nd Stage: Learn 2nd Level Feature From 1st Level Feature





Stacked Autoencoder

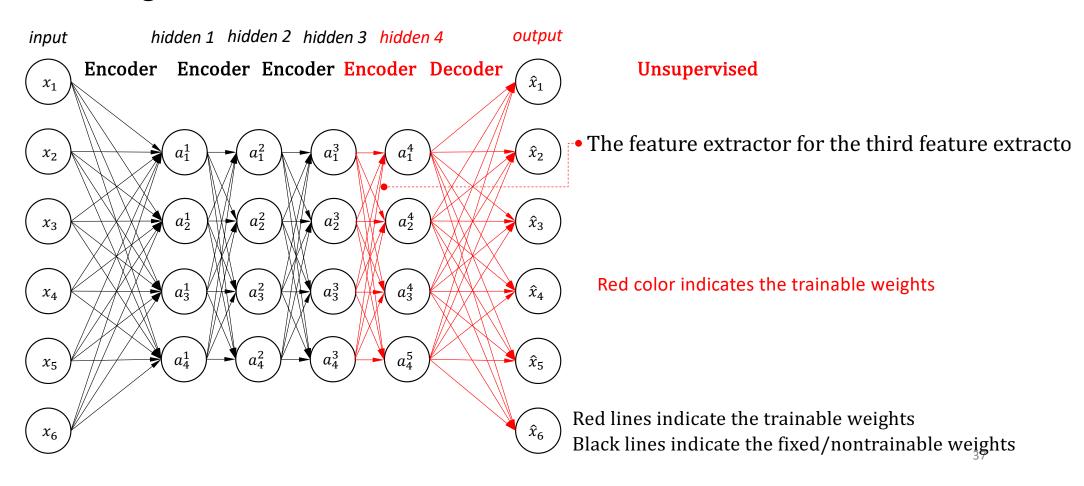
3rd Stage: Learn 3rd Level Feature From 2nd Level Feature





Stacked Autoencoder

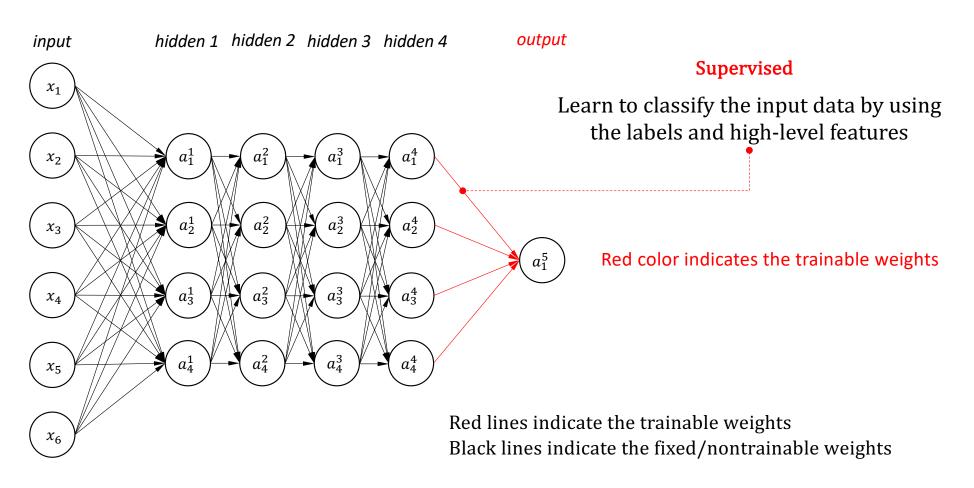
• 4th Stage: Learn 4th Level Feature From 3rd Level Feature





Stacked Autoencoder

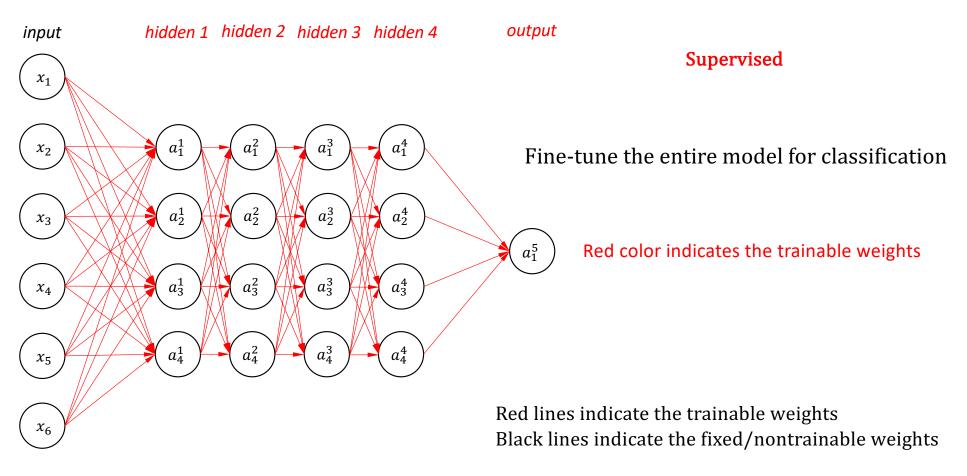
Use the Learned Feature Extractor for Downstream Tasks





Stacked Autoencoder

Fine-tuning







Discussion

- Advantages
 - ...

- Disadvantages
 - ...



- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)
 - From Neural Network Perspective
 - From Probability Model Perspective

和桌头灣 PEKING UNIVERSITY

Before we start

- Question?
 - Are the previous Autoencoders generative model?
 - Recap: We want to learn a probability distribution p(x) over x
 - O Generation (sampling): $\mathbf{x}_{new} \sim p(\mathbf{x})$ (NO, The compressed latent codes of autoencoders are not prior distributions, autoencoder cannot learn to represent the data distribution)
 - O Density Estimation: p(x) high if x looks like a real data NO
 - Unsupervised Representation Learning:

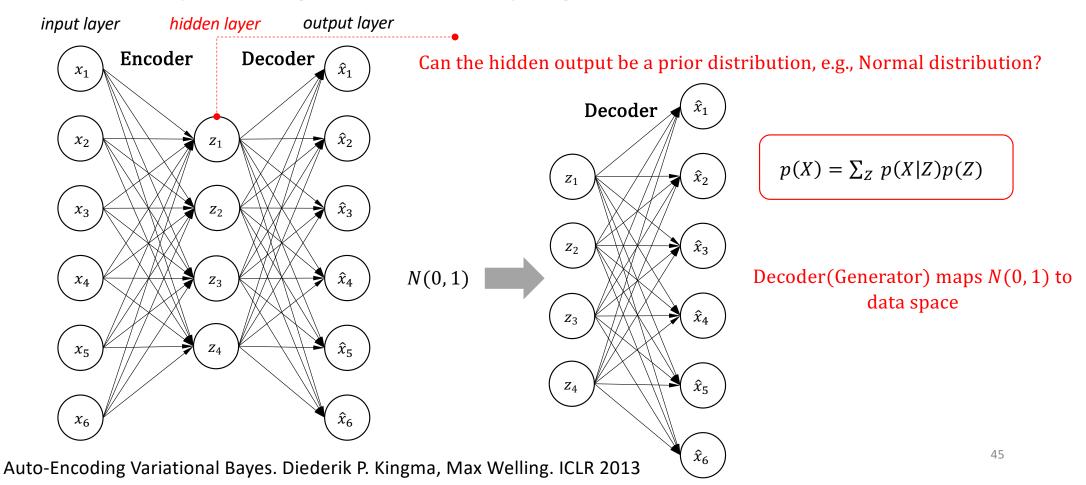
Discovering the underlying structure from the data distribution (e.g., ears, nose, eyes ...) (YES, Autoencoders learn the feature representation)



- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)
 - From Neural Network Perspective
 - From Probability Model Perspective

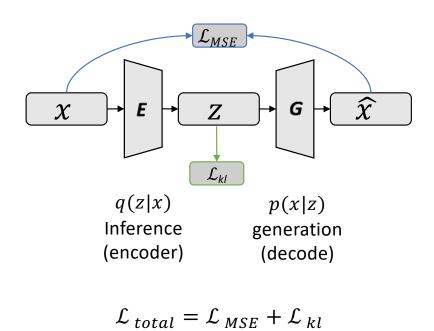


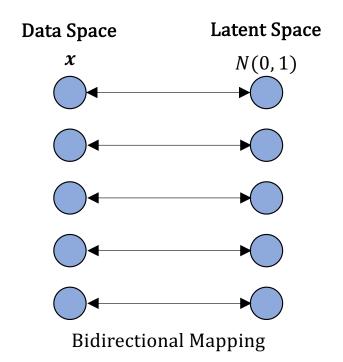
How to perform generation (sampling)?





Quick Overview







- The neural net perspective
 - A variational autoencoder consists of an encoder, a decoder, and a loss function



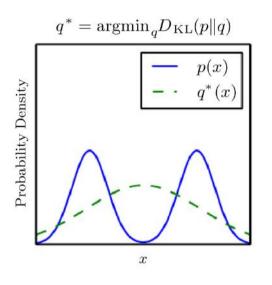
Loss function

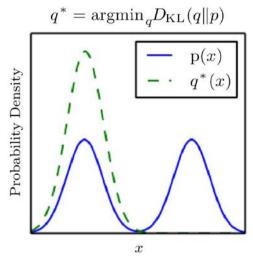
$$l_i(heta,\phi) = -\mathbb{E}_{z\sim q_{ heta}(z|x_i)}[\log p_{\phi}(x_i\mid z)] + \mathbb{KL}(q_{ heta}(z\mid x_i)\mid\mid p(z))$$

Can be represented by MSE

regularisation

Why KL(Q||P) not KL(P||Q)





Which direction of the KL divergence to ensure
 use?

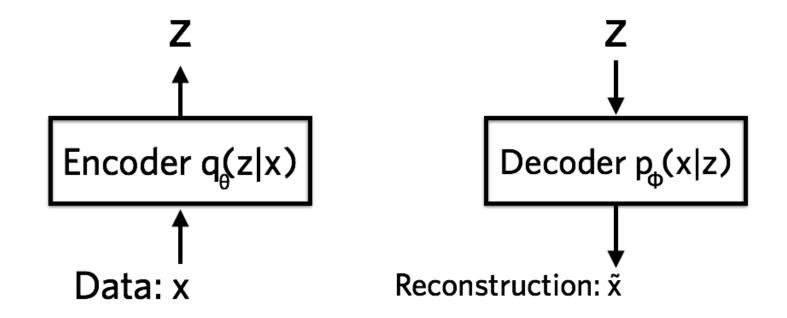
加京大学

- Some applications require an approximation that usually places high probability anywhere that the true distribution places high probability: left one
- VAE requires an approximation that rarely places high probability anywhere that the true distribution places low probability: right one

If:
$$D_{\mathrm{KL}}(P\|Q) = \mathbb{E}_{\mathbf{x} \sim P} \left[\log \frac{P(x)}{Q(x)} \right] = \mathbb{E}_{\mathbf{x} \sim P} \left[\log P(x) - \log Q(x) \right].$$

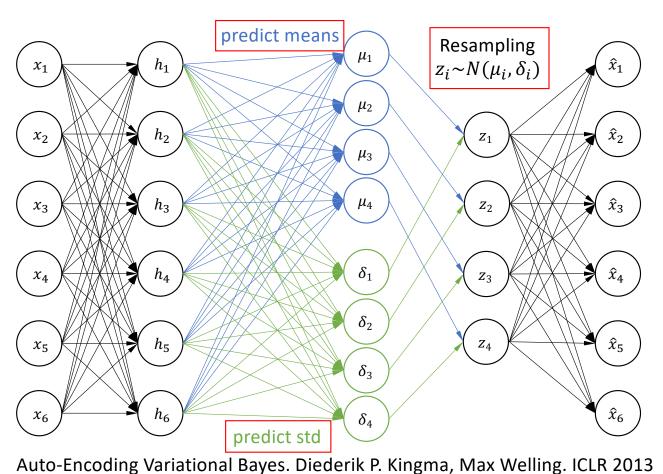


• Encoder, Decoder





Reparameterisation Trick



- 1. Encode the input
- 2. Predict means
- 3. Predict standard derivations
- 4. Use the predicted means and standard derivations to sample new latent variables individually
- 5. Reconstruct the input



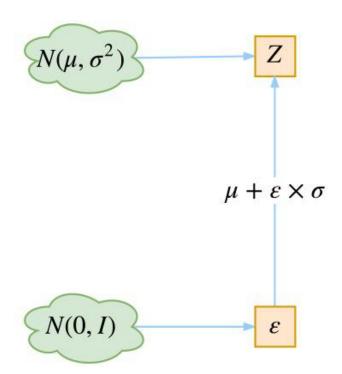
Reparameterisation Trick

- $z \sim N(\mu, \sigma)$ is not differentiable
- To make sampling z differentiable

•
$$z = \mu + \sigma * \in \sim N(0, 1)$$

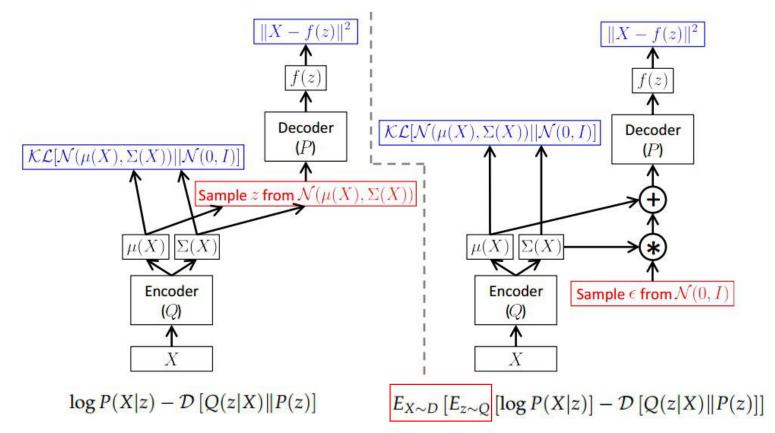
$$\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(z-\mu)^2}{2\sigma^2}\right) dz$$

$$= \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{z-\mu}{\sigma}\right)^2\right] d\left(\frac{z-\mu}{\sigma}\right)$$





Reparameterisation Trick





Loss function

$$\mathbb{KL}(q_{ heta}(z\mid x_i)\mid\mid p(z))$$



Where is 'variational'?

$$\mathbb{KL}(q_{ heta}(z\mid x_i)\mid\mid p(z))$$



- Vanilla Autoencoder
- Denoising Autoencoder
- Sparse Autoencoder
- Contractive Autoencoder
- Stacked Autoencoder
- Variational Autoencoder (VAE)
 - From Neural Network Perspective
 - From Probability Model Perspective



Problem Definition

Goal: Given $X = \{x_1, x_2, x_3 \dots, x_n\}$, find p(X) to represent X

How: It is difficult to directly model p(X), so alternatively, we can ...

$$p(X) = \sum_{Z} p(X|Z)p(Z)$$

where p(Z) = N(0,1) is a prior/known distribution

i.e., sample X from Z



- The probability model perspective
 - P(X) is hard to model

$$p(X) = \sum_{Z} p(X|Z)p(Z)$$

Alternatively, we learn the joint distribution of X and Z

$$p(X,Z) = p(Z)p(X|Z)$$

$$p(X) = \sum_{Z} p(X, Z)$$

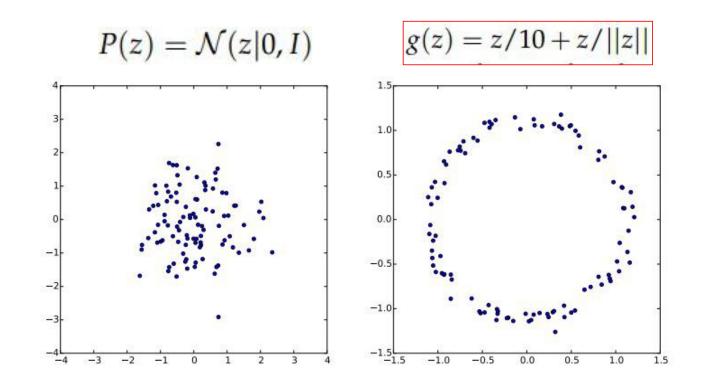


Assumption

$$P(z) = \mathcal{N}(z|0, I)$$



Assumption



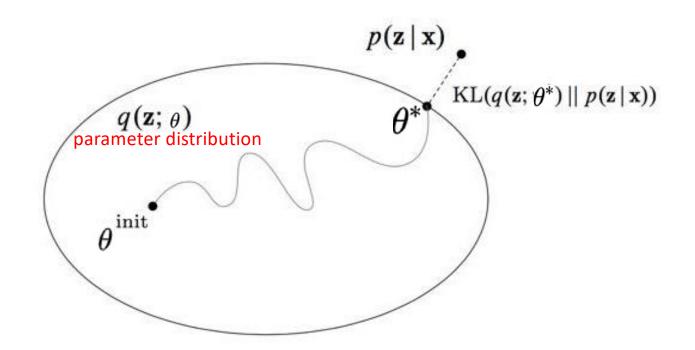


- Recap: Variational Inference
 - VI turns inference into optimisation

$$p(x) = \int p(x,z) \mathrm{d}z$$
 $\mathcal{D} = \{q_{ heta}(z)\}$ $heta^* = rg \min_{ heta} egin{array}{c} \mathsf{KL}(q_{ heta}(z) \parallel p(z|x)) & p(z|x) = rac{p(x,z)}{p(x)} & p(x,z) \end{pmatrix}$ $heta^* = rg \max_{ heta} \mathbb{E}_q[\log p(x,z) - \log q_{ heta}(z)]$



- Variational Inference
 - VI turns inference into optimisation





- Setting up the objective
 - Maximise P(X)
 - Set Q(z) to be an arbitrary distribution

$$p(z|X) = \frac{p(X|z)p(z)}{p(X)}$$

$$\mathcal{D}\left[Q(z)\|P(z|X)\right] = E_{z \sim Q}\left[\log Q(z) - \log P(z|X)\right]$$

$$\mathcal{D}[Q(z)||P(z|X)] = E_{z \sim Q}[\log Q(z) - \log P(X|z) - \log P(z)] + \log P(X)$$

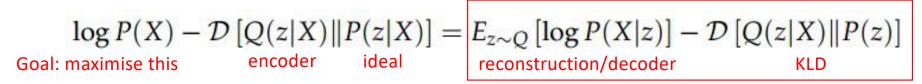
$$\log P(X) - \mathcal{D}[Q(z)||P(z|X)] = E_{z \sim Q}[\log P(X|z)] - \mathcal{D}[Q(z)||P(z)]$$

$$\log P(X) - \mathcal{D}[Q(z|X)||P(z|X)] = E_{z \sim Q}[\log P(X|z)] - \mathcal{D}[Q(z|X)||P(z)]$$

Goal: maximise this logP(x)

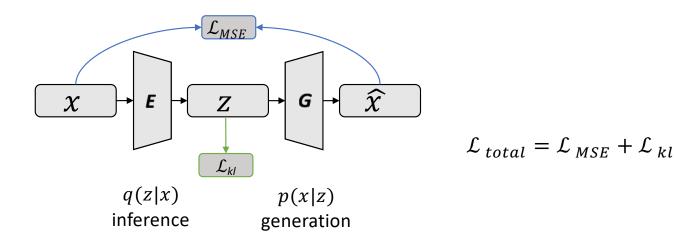


Setting up the objective



difficult to compute

Goal becomes: optimize this





Setting up the objective : ELBO (Evidence Lower Bound)

$$\mathcal{D}_{l}(Q(z \mid x) \mid\mid P(z \mid x)) = \frac{p(X,z)}{p(X)}$$

$$\mathbf{E}_{q}[\log Q(z \mid x)] - \mathbf{E}_{q}[\log P(x,z)] + \log P(x)$$

$$\mathbf{E}_{l}(z \mid x) = \arg\min_{\theta} \mathcal{D}_{l}(Q(z \mid x) \mid\mid P(z \mid x))$$

$$ELBO(\theta) = \mathbf{E}_{q}[\log P(x,z)] - \mathbf{E}_{q}[\log Q(z \mid x)]$$



Recap: The KL Divergence Loss

$$|Vergence Loss|_{KL(\mathcal{N}(\mu,\sigma^2)||\mathcal{N}(0,1))} = \int \mathcal{N}(\mu,\sigma^2) \log \frac{\mathcal{N}(\mu,\sigma^2)}{\mathcal{N}(0,1)} dx$$

$$= \int \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \left(\log \frac{\frac{1}{\sqrt{2\pi\sigma^2}}}{\frac{1}{\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}} \right) dx$$

$$= \int \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \log \left(\frac{1}{\sqrt{\sigma^2}} e^{\frac{x^2 - (x-\mu)^2}{2\sigma^2}} \right) dx$$

$$= \frac{1}{2} \int \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \left[-\log \sigma^2 + x^2 - \frac{(x-\mu)^2}{\sigma^2} \right] dx$$



Recap: The KL Divergence Loss

$$= \frac{1}{2} \int \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \left[-\log\sigma^2 + x^2 - \frac{(x-\mu)^2}{\sigma^2} \right] dx$$

$$= \frac{1}{2} \left(-\log\sigma^2 + \mu^2 + \sigma^2 - 1 \right)$$



Recap: The KL Divergence Loss

$$\mathcal{D}[\mathcal{N}(\mu_0, \Sigma_0) || \mathcal{N}(\mu_1, \Sigma_1)] = \frac{1}{2} \left(\operatorname{tr} \left(\Sigma_1^{-1} \Sigma_0 \right) + (\mu_1 - \mu_0)^\top \Sigma_1^{-1} (\mu_1 - \mu_0) - k + \log \left(\frac{\det \Sigma_1}{\det \Sigma_0} \right) \right)$$



Optimising the objective

$$\log P(X) - \mathcal{D}\left[\underset{\text{encoder ideal}}{Q(z|X)} \| P(z|X) \right] = E_{z \sim Q}\left[\log P(X|z)\right] - \mathcal{D}\left[\underset{\text{reconstruction}}{Q(z|X)} \| P(z) \right]$$

$$E_{X \sim D} \begin{bmatrix} \log P(X) - \mathcal{D} \left[Q(z|X) \| P(z|X) \right] \right] = \\ E_{X \sim D} \\ \operatorname{dataset} \end{bmatrix} [E_{Z \sim Q} \left[\log P(X|z) \right] - \mathcal{D} \left[Q(z|X) \| P(z) \right]]$$



VAE is a Generative Model

p(Z|X) is not N(0,1)

Can we input N(0,1) to the decoder for sampling?

YES: the goal of KL is to make p(Z|X) to be N(0,1)



- VAE vs. Autoencoder
 - VAE : distribution representation, p(z|x) is a distribution
 - AE: feature representation, h = E(x) is deterministic



Challenges

Low quality images

• ..



Summary: Take Home Message

- Autoencoders learn data representation in an unsupervised/ self-supervised way.
- Autoencoders learn data representation but cannot model the data distribution p(X).
- Different with vanilla autoencoder, in sparse autoencoder, the number of hidden units can be greater than the number of input variables.
- VAE
- ...
- ...
- ...
- ...
- ...
- ..



Thanks