

Fundamentals of Probabilistic Data Mining

Chapter VI - Variational Autoencoders (VAE)

Xavier Alameda-Pineda

Why does the EM work?

The main mathematical object in EM is \mathcal{Q} .

(The expected complete-data log-likelihood).

What is the relationship with the log-likelihood?

Let's take any distribution of \mathbf{z} : $q(\mathbf{z})$ and ignore Θ for the time being.

$$\log p(\mathbf{x}) = \mathbb{E}_{q(\mathbf{z})} \left\{ \log p(\mathbf{x}) \right\} \quad (1)$$

$$= \mathbb{E}_{q(\mathbf{z})} \left\{ \log p(\mathbf{x}) \frac{p(\mathbf{z}|\mathbf{x})q(\mathbf{z})}{p(\mathbf{z}|\mathbf{x})q(\mathbf{z})} \right\} \quad (2)$$

$$= \mathbb{E}_{q(\mathbf{z})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z})}{q(\mathbf{z})} \right\} + D_{\text{KL}}(q(\mathbf{z}) \parallel p(\mathbf{z}|\mathbf{x})) \quad (3)$$

Why does the EM work? (II)

$$\log p(\mathbf{x}; \Theta) = \underbrace{\mathbb{E}_{q(\mathbf{z})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z})}{q(\mathbf{z})} \right\}}_{\text{M-step}} + \underbrace{D_{\text{KL}}(q(\mathbf{z}) \parallel p(\mathbf{z}|\mathbf{x}))}_{\text{E-step}} \quad (4)$$

Another interpretation. Given $\bar{\Theta}$:

① Set $q(\mathbf{z}) = p(\mathbf{z}|\mathbf{x}; \bar{\Theta})$.

② Optimise w.r.t. Θ :

$$\mathbf{E}_{q(\mathbf{z})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z}; \Theta)}{q(\mathbf{z})} \right\} \quad (5)$$

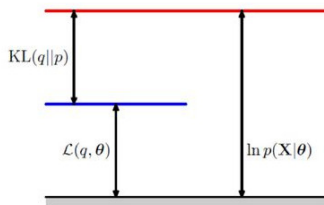
Why?

E-step: reduce the distance between log-likelihood and \mathcal{Q} .

M-step: push \mathcal{Q} and therefore push the log-likelihood.

Why does the EM work? (III)

$$\log p(\mathbf{x}; \Theta) = \underbrace{\mathbb{E}_{q(\mathbf{z})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z})}{q(\mathbf{z})} \right\}}_{\mathcal{L}(q, \Theta)} + \underbrace{D_{\text{KL}}(q(\mathbf{z}) \parallel p(\mathbf{z}|\mathbf{x}))}_{\text{KL}(q \parallel p)} \quad (6)$$



Crucial point in “Exact EM”

We **need** the exact a posteriori distribution: $p(\mathbf{z}|\mathbf{x}; \bar{\Theta})$.

What happens if we cannot use the exact posterior? **Approximate it.**

Two big families:

- $p(\mathbf{z}|\mathbf{x}; \bar{\Theta})$ has an analytic expression, but computationally too heavy.
- $p(\mathbf{z}|\mathbf{x}; \bar{\Theta})$ does not have an analytic expression.

We will focus in the second case, and in a model called **Variational Autoencoders (VAE)**.

VAE Motivation: back to PPCA

Recall the definition of PPCA:

- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$,
- $\mathbf{x}|\mathbf{z} \sim \mathcal{N}(\mathbf{x}; \mathbf{A}\mathbf{z} + \mathbf{b}, \sigma^2\mathbf{I})$, $\sigma > 0$.

Important limitations:

- The dependency of the mean with \mathbf{z} is **affine**.
- The covariance does not depend on \mathbf{z} .

Non-linear generative model:

- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$,
- $\mathbf{x}|\mathbf{z} \sim \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z}))$,

where $\boldsymbol{\mu}_{\Theta}(\mathbf{z})$ and $\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})$ are (non-linear) functions parametrised by Θ .

Formalising the generative model (I)

The generative model:

- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$,
- $\mathbf{x}|\mathbf{z} \sim \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z}))$,

where $\boldsymbol{\mu}_{\Theta}(\mathbf{z})$ and $\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})$ will be implemented **by deep neural networks** parametrised by Θ with input \mathbf{z} .

Formalising the generative model (I)

The generative model:

- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$,
- $\mathbf{x}|\mathbf{z} \sim \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z}))$,

where $\boldsymbol{\mu}_{\Theta}(\mathbf{z})$ and $\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})$ will be implemented **by deep neural networks** parametrised by Θ with input \mathbf{z} .

A few comments:

- ① The optimal parameters Θ^* need to maximise the log-likelihood.
- ② Θ cannot be estimated in closed-form.
- ③ $\boldsymbol{\mu}_{\Theta}(\mathbf{z})$ and $\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})$ are differentiable w.r.t. Θ , and \mathbf{z} .
- ④ $\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})$ needs to be a covariance matrix.

Formalising the generative model (II)

How can we ensure that $\Sigma_{\Theta}(\mathbf{z})$ is a covariance matrix?

- The covariance matrix is assumed to be diagonal:

$$\Sigma_{\Theta}(\mathbf{z}) = \begin{pmatrix} \nu_{\Theta}^{(1)}(\mathbf{z}) & 0 & \cdots & 0 \\ 0 & \nu_{\Theta}^{(2)}(\mathbf{z}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \nu_{\Theta}^{(D)}(\mathbf{z}) \end{pmatrix} \quad (7)$$

Reduces complexity and memory, but also expressivity.

- We estimate the log-variance: $\eta_{\Theta}^{(d)}(\mathbf{z}) = \log \nu_{\Theta}^{(d)}(\mathbf{z})$:

$$\Sigma_{\Theta}(\mathbf{z}) = \text{diag}_d \left(\exp \left(\eta_{\Theta}^{(d)}(\mathbf{z}) \right) \right) \quad (8)$$

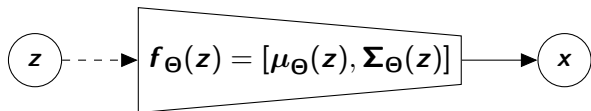
The values of $\eta_{\Theta}^{(d)}(\mathbf{z})$ can be positive or negative.

Formalising the generative model (III)

In terms of probabilistic dependencies, they are the same as PPCA:



But I would like to draw also the non-linearity:



The dependency of the parameters w.r.t. \mathbf{z} is **deterministic**.

Denoted by $\mathbf{f}_{\Theta}(\mathbf{z}) : \mathbb{R}^{d_z} \rightarrow \mathbb{R}^{2d_x}$, this non-linearity is implemented with a deep network, with parameters (weights and biases) Θ .

The posterior distribution

For any EM-like procedure, we would need the posterior distribution:

$$p(\mathbf{z}|\mathbf{x}) \stackrel{(z)}{\propto} p(\mathbf{x}|\mathbf{z})p(\mathbf{z}) \quad (9)$$

$$\stackrel{(z)}{\propto} \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z}))\mathcal{N}(\mathbf{z}; \mathbf{0}, I) \quad (10)$$

$$\stackrel{(z)}{\propto} \frac{1}{|\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})|^{1/2}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\Theta}(\mathbf{z}))^{\top} \boldsymbol{\Sigma}_{\Theta}^{-1}(\mathbf{z})(\mathbf{x} - \boldsymbol{\mu}_{\Theta}(\mathbf{z})) - \frac{1}{2}\|\mathbf{z}\|^2\right) \quad (11)$$

The posterior distribution

For any EM-like procedure, we would need the posterior distribution:

$$p(\mathbf{z}|\mathbf{x}) \stackrel{(z)}{\propto} p(\mathbf{x}|\mathbf{z})p(\mathbf{z}) \quad (9)$$

$$\stackrel{(z)}{\propto} \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z}))\mathcal{N}(\mathbf{z}; \mathbf{0}, I) \quad (10)$$

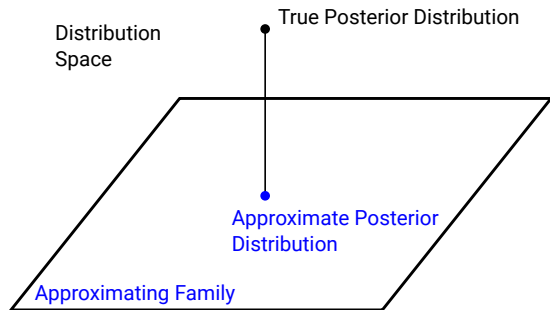
$$\stackrel{(z)}{\propto} \frac{1}{|\boldsymbol{\Sigma}_{\Theta}(\mathbf{z})|^{1/2}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\Theta}(\mathbf{z}))^{\top} \boldsymbol{\Sigma}_{\Theta}^{-1}(\mathbf{z})(\mathbf{x} - \boldsymbol{\mu}_{\Theta}(\mathbf{z})) - \frac{1}{2}\|\mathbf{z}\|^2\right) \quad (11)$$

We cannot go our “standard” way, because we cannot identify a distribution on \mathbf{z} .

The posterior distribution cannot be computed analytically!!!

Approximating the posterior distribution (I)

The posterior distribution needs to be approximated. We will propose a family of distributions, and find the **best candidate within this family**.



Approximating the posterior distribution (II)

The posterior distribution will be approximated with **another** feed-forward network parametrised with Φ :

$$p(\mathbf{z}|\mathbf{x}) \approx q(\mathbf{z}|\mathbf{x}) = \mathcal{N}(\mathbf{z}; \tilde{\boldsymbol{\mu}}_{\Phi}(\mathbf{x}), \tilde{\boldsymbol{\Sigma}}_{\Phi}(\mathbf{x})) \quad (12)$$

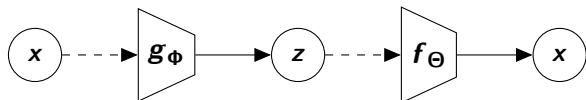
The approximating family is composed of all the distributions that can be expressed as above, for a certain value of Φ .

$$\mathcal{G} = \{\mathbf{g}_{\Phi} : \mathbb{R}^{d_x} \rightarrow \mathbb{R}^{2d_z}; \Phi \in \Phi\}, \quad (13)$$

with $\mathbf{g}_{\Phi}(\mathbf{x}) = [\tilde{\boldsymbol{\mu}}_{\Phi}(\mathbf{x}), \tilde{\boldsymbol{\Sigma}}_{\Phi}(\mathbf{x})]$.

Overall architecture

If we “chain” the posterior and the generative model:



- The generative model is also called the **decoder**.
- The inference or posterior is also called the **encoder**.

This is why we call these architectures **variational autoencoders** VAE.

But how do we optimise for the parameters Θ and Φ ?

Learning - ELBO

If we recall the formulation for the EM:

$$\log p(\mathbf{x}) = \mathbb{E}_{q(\mathbf{z}|\mathbf{x})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z})}{q(\mathbf{z}|\mathbf{x})} \right\} + D_{\text{KL}}(q(\mathbf{z}|\mathbf{x}) \parallel p(\mathbf{z}|\mathbf{x})) \quad (14)$$

Problem: the second term cannot be computed! But it's positive:

$$\log p(\mathbf{x}; \Theta, \Phi) \geq \mathbb{E}_{q_{\Phi}(\mathbf{z}|\mathbf{x})} \left\{ \log \frac{p(\mathbf{x}, \mathbf{z})}{q_{\Phi}(\mathbf{z}|\mathbf{x})} \right\} \quad (15)$$

$$\log p(\mathbf{x}; \Theta, \Phi) \geq \underbrace{\mathbb{E}_{q_{\Phi}(\mathbf{z}|\mathbf{x})} \left\{ \log p_{\Theta}(\mathbf{x}|\mathbf{z}) \right\}}_{\text{Reconstruction}} - \underbrace{D_{\text{KL}}(q_{\Phi}(\mathbf{z}|\mathbf{x}) \parallel p(\mathbf{z}))}_{\text{Regularisation}} \quad (16)$$

This is known as **Evidence Lower-BOund or ELBO**: $\mathcal{L}_{\text{ELBO}}(\Theta, \Phi)$.

Be VERY careful with these expressions.

They look alike, but they are NOT the same.

Learning - Sampling

But we still have one problem:

$$\mathcal{L}_{\text{ELBO}}(\Theta, \Phi) = \underbrace{\mathbb{E}_{q_{\Phi}(\mathbf{z}|\mathbf{x})} \left\{ \log p_{\Theta}(\mathbf{x}|\mathbf{z}) \right\}}_{\text{Reconstruction}} - \underbrace{D_{\text{KL}}(q_{\Phi}(\mathbf{z}|\mathbf{x}) \parallel p(\mathbf{z}))}_{\text{Regularisation}} \quad (17)$$

To compute the “reconstruction” term we need to take the expectation w.r.t. $q_{\Phi}(\mathbf{z}|\mathbf{x})$, but recall that:

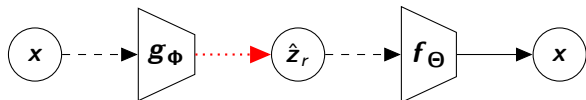
$$p_{\Theta}(\mathbf{x}|\mathbf{z}) = \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_{\Theta}(\mathbf{z}), \boldsymbol{\Sigma}_{\Theta}(\mathbf{z})). \quad (18)$$

Due to the non-linearity, we cannot compute the reconstruction term in closed form \rightarrow we sample R points $\hat{\mathbf{z}}_1, \dots, \hat{\mathbf{z}}_R$ from q_{Φ} :

$$\mathcal{L}_{\text{ELBO}}(\Theta, \Phi) = \underbrace{\frac{1}{R} \sum_{r=1}^R \log p_{\Theta}(\mathbf{x}|\hat{\mathbf{z}}_r)}_{\text{Reconstruction}} - \underbrace{D_{\text{KL}}(q_{\Phi}(\mathbf{z}|\mathbf{x}) \parallel p(\mathbf{z}))}_{\text{Regularisation}} \quad (19)$$

Learning - Gradient ascent?

Let's go back to the architecture:



where dashed lines are deterministic, dotted lines are sampling (we will see later for the solid line).

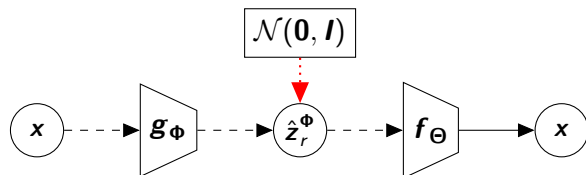
We agreed that there is no closed-form solution for the parameters (due to non-linearity). We will learn the parameters using stochastic gradient ascent (to maximise the ELBO).

We assume that g_{Φ} and f_{Θ} are differentiable (to compute the gradient).

The sampling operation from q_{Φ} is **NOT** differentiable w.r.t. Φ .

Learning - Reparametrisation trick

We use the so-called **reparametrisation trick**:



Formally (\hat{z}_r^{Φ} denotes explicitly the dependency on Φ):

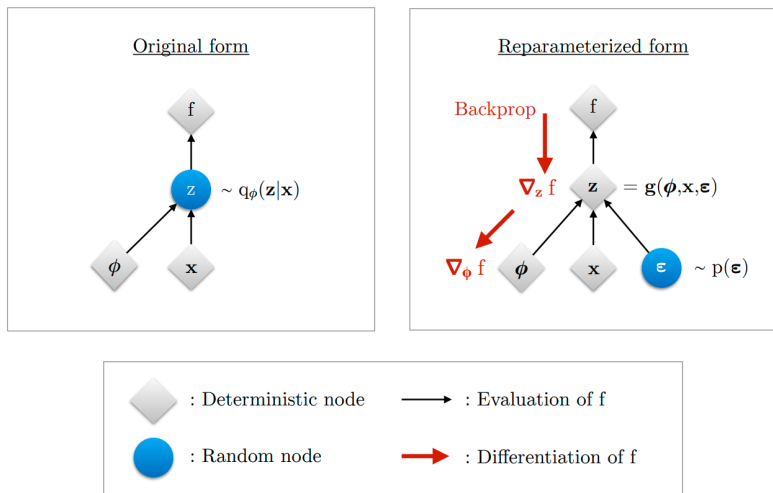
$$\hat{z}_r^{\Phi} = \tilde{\Sigma}_{\Phi}^{1/2} \hat{\epsilon}_r + \tilde{\mu}_{\Phi} \quad \text{with} \quad \hat{\epsilon}_r \sim \mathcal{N}(\mathbf{0}, I) \quad (20)$$

So we sample from a standard Gaussian, and use the parameters $\tilde{\mu}_{\Phi}$ and $\tilde{\Sigma}_{\Phi}$ in **differentiable operations** (multiplication and addition).

If the last arrow is differentiable, then we can use gradient ascent.

Learning - Reparametrisation trick (II)

Another way to see the reparametrisation trick (from “An Introduction to Variational Autoencoders” by Diederik P. Kingma, Max Welling, [chamilo](#)):



Learning - The loss

We are now ready to write the loss:

$$\mathcal{L}_{\text{ELBO}}(\Theta, \Phi) = \underbrace{\mathbb{E}_{q_{\Phi}(z|\mathbf{x})} \left\{ \log p_{\Theta}(\mathbf{x}|z) \right\}}_{\text{Reconstruction}} - \underbrace{D_{\text{KL}}(q_{\Phi}(z|\mathbf{x}) \parallel p(z))}_{\text{Regularisation}} \quad (21)$$

$$= \underbrace{\sum_{r=1}^R \log p_{\Theta}(\mathbf{x}|\hat{\mathbf{z}}_r^{\Phi})}_{\text{Reconstruction}} - \underbrace{D_{\text{KL}}(q_{\Phi}(z|\mathbf{x}) \parallel p(z))}_{\text{Regularisation}} \quad (22)$$

$$\stackrel{(\Theta, \Phi)}{=} -\frac{1}{2} \left[\frac{1}{R} \sum_{r=1}^R \left(\log |\Sigma_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})| + \|\mathbf{x} - \mu_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})\|_{\Sigma_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})}^2 \right) \right] \quad (23)$$

$$+ \text{Tr}(\Sigma_{\Phi}(\mathbf{x})) + \|\mu_{\Phi}(\mathbf{x})\|^2 - \log |\Sigma_{\Phi}(\mathbf{x})| \quad (24)$$

Where (23) and (24) are the reconstruction and regularisation terms resp.

Homework: use the definition of the terms above to prove that.

Learning - The loss (II)

$$\mathcal{L}_{\text{ELBO}}(\Theta, \Phi) \stackrel{(\Theta, \Phi)}{=} -\frac{1}{2} \left[\frac{1}{R} \sum_{r=1}^R \left(\log |\Sigma_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})| + \|\mathbf{x} - \mu_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})\|_{\Sigma_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})}^2 \right) \right] \quad (25)$$

$$+ \text{Tr}(\Sigma_{\Phi}(\mathbf{x})) + \|\mu_{\Phi}(\mathbf{x})\|^2 - \log |\Sigma_{\Phi}(\mathbf{x})| \quad (26)$$

Comments:

- We recall that $\hat{\mathbf{z}}_r^{\Phi} = \tilde{\Sigma}_{\Phi}^{1/2} \hat{\epsilon}_r + \tilde{\mu}_{\Phi}$ with $\hat{\epsilon}_r \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$.
- We remark that all operators are differentiable w.r.t. Θ and Φ .
- If we remove the “ $-\frac{1}{2}$ ” we use gradient descent.
- The term in blue is the **Mahalanobis distance** and can be replaced...

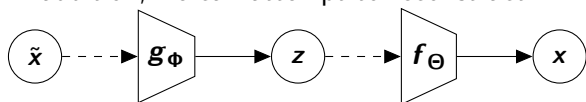
Other reconstruction possibilities

Often, we forget about the covariance matrix of the generative model Σ_{Θ} and use other distances rather than Mahalanobis:

- The Euclidean distance (equivalent to set $\Sigma_{\Theta} = I$): $\|\mathbf{x} - \mu_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})\|_2^2$
- The L_1 distance: $\|\mathbf{x} - \mu_{\Theta}(\hat{\mathbf{z}}_r^{\Phi})\|_1$
- ...

In that case $\mathbf{f}_{\Theta}(\mathbf{z}) : \mathbb{R}^{d_z} \rightarrow \mathbb{R}^{d_x}$ (instead of \mathbb{R}^{2d_x}), and this links to the deterministic autoencoders.

In addition, we can attempt to reconstruct \mathbf{x} from another signal $\tilde{\mathbf{x}}$:



a clear example are denoising VAE ($\tilde{\mathbf{x}} = \mathbf{x} + \mathbf{b}$, with \mathbf{b} being noise).

Differences w.r.t. EM

[EM]: Start with $\bar{\Theta}$:

- E-step: Compute $p(\mathbf{z}_n | \mathbf{x}_n; \bar{\Theta})$, $\forall n$.
- M-step: Compute Θ^* , and set $\bar{\Theta}$ to that.

(Until convergence)

[SGD]: Start with $\bar{\Theta}$. Initialise also $\bar{\Phi}$:

- Forward: Compute $\mathbf{g}_{\bar{\Phi}}(\mathbf{x}_n)$, sample \mathbf{z}_n , compute $\mathbf{f}_{\bar{\Theta}}(\mathbf{z}_n)$, $\forall n$ in batch.
- Backward: Compute $\mathcal{L}_{\text{ELBO}}$, $\nabla_{\bar{\Theta}} \mathcal{L}_{\text{ELBO}}$, and $\nabla_{\bar{\Phi}} \mathcal{L}_{\text{ELBO}}$.
- Update $\bar{\Theta}$ and $\bar{\Phi}$ with your preferred gradient update rule.

(Until convergence)

