Machine Learning for Data Science (CS 4786)

Lecture 9: Principal Component Analysis

The text in black outlines main ideas to retain from the lecture. The text in blue give a deeper understanding of how we "derive" or get to the algorithm or method. The text in red are mathematical details for those who are interested. But is not crucial for understanding the basic workings of the method.

1 Dimensionality Reduction and Linear Projection

We are provided with data points $\mathbf{x}_1, \ldots, \mathbf{x}_n$ where each $\mathbf{x}_t \in \mathbb{R}^d$ is a d-dimensional vector. The goal is to compress these points into vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathbb{R}^K$ where K is smaller than d.

In this lecture we will consider the method of Principal Components Analysis which is a method based on linear projection. In any linear projection/transformation based method, given any $\mathbf{x}_t \in \mathbb{R}^d$ we obtain the corresponding low dimensional representation $\mathbf{y}_t \in \mathbb{R}^k$ as

$$\mathbf{y}_t^\top = \mathbf{x}_t^\top W$$

where W is a $d \times K$ matrix. Notice that one can represent the matrix W as

$$W = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$$

where $\mathbf{w}_1, \ldots, \mathbf{w}_K$ are each d-dimensional vectors. Data matrix X of size $n \times d$ has as its rows, $\mathbf{x}_t^\top$.

2 Orthonormal Basis and Projections

Before we proceed, note that if all the points $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are translated as a group, this should not affect how well we can compress the points. All we really care about is the location of these points relative to each other. In view of this, to make the compression scheme translation invariant, we shall always center the points. Specifically we shall compute the sample mean of the n points

$$\boldsymbol{\mu} = \frac{1}{n}\sum_{t=1}^{n} \mathbf{x}_t$$

and our goal will be to compress $\mathbf{x}_1 - \boldsymbol{\mu}, \ldots, \mathbf{x}_n - \boldsymbol{\mu}$ instead.

A simple fact from linear algebra is that, if we consider any orthonormal basis of $\mathbb{R}^d$ given by $\mathbf{w}_1, \ldots, \mathbf{w}_d \in \mathbb{R}^d$, then any vector in $\mathbb{R}^d$ can be represented as a linear combination of the d basis. Recall that orthonormal vectors are vectors $\mathbf{w}_1, \ldots, \mathbf{w}_d$ such that each vector is of unit length, that is

$$\forall i \leq d, \qquad \|\mathbf{w}_i\|_2^2 = \sum_{j=1}^{d} \mathbf{w}_i[j]^2 = 1$$

and the vectors are orthogonal to each other, that is

$$\forall i, j \text{ s.t. } i \neq j, \quad \mathbf{w}_i^\top \mathbf{w}_j = 0$$

The key idea we are going to use to produce the K dimensional representation of the n points is that we shall first find orthonormal basis $\mathbf{w}_1, \ldots, \mathbf{w}_d$ in which to represent each point $\mathbf{x}_t - \boldsymbol{\mu}$. But however we shall pick only K of the d basis $\mathbf{w}_1, \ldots, \mathbf{w}_d$ and represent the points in the chosen K dimensional subspace spanned by $\mathbf{w}_1, \ldots, \mathbf{w}_K$. Thus the matrix W will be got by considering only these K basis.

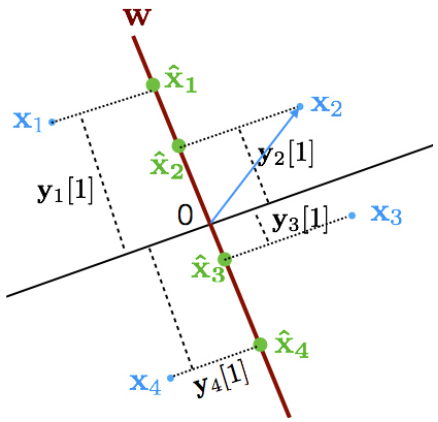
Since we can write any vector in d-dimension as a linear combination of the orthonormal basis, let us write each

$$\mathbf{x}_t - \boldsymbol{\mu} = \sum_{j=1}^{d} \mathbf{y}_t[j] \mathbf{w}_j \tag{1}$$

where for each $\mathbf{x}_t$, $\mathbf{y}_t[j]$ represents the coefficient on the jth basis $\mathbf{w}_j$. Now the K dimensional representation of the point $\mathbf{x}_t$ is given by the K numbers $\mathbf{y}_t[1], \ldots, \mathbf{y}_t[K]$. What this means is that we can view the data point $\mathbf{x}_t$ being approximated by the reconstruction

$$\hat{\mathbf{x}}_t = \sum_{j=1}^{K} \mathbf{y}_t[j] \mathbf{w}_j + \boldsymbol{\mu} \tag{2}$$

The figure below illustrates the basic idea. The points in blue are the original $\mathbf{x}_1, \ldots, \mathbf{x}_n$. The orthonormal basis chosen is illustrated in the figure and the red line (basis) is the one dimension we retain and the other one is thrown away. The points in green represent the reconstructions $\hat{\mathbf{x}}_1, \ldots, \hat{\mathbf{x}}_n$. The one dimensional representation $\hat{\mathbf{y}}_1[1], \ldots, \hat{\mathbf{y}}_n[1]$ are illustrated by the lengths in the figure.



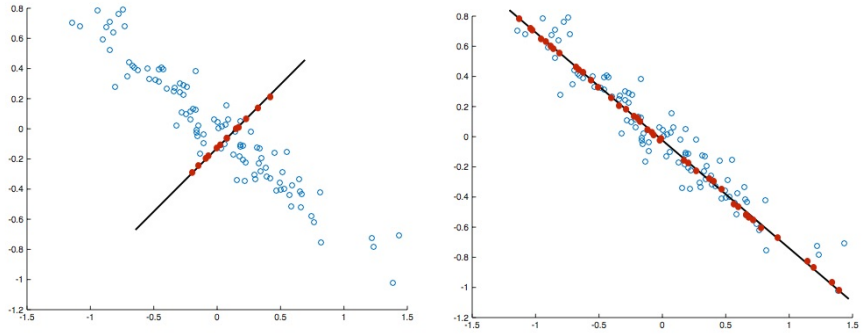
$$\mathbf{y_2}[1] = \mathbf{x}_1^\top \mathbf{w} = \|\mathbf{x_2}\| \cos(\angle \mathbf{xw})$$

Now the main question at hand boils down to, ***How do we pick the right orthonormal basis, and which of the basis do we retain/ throw away.***

3 View I: Variance Maximization

Basic idea: Pick the directions along which data is maximally spread (or variance is high).

As en example in the illustration below we would like to pick the second option as the spread if the points across the chosen direction is larger in the second figure.



How do we formalize this?

Let us first consider the first direction to pick $\mathbf{w}_1$. We want to pick the direction long which variance of $\hat{y}_1[1], \ldots, \hat{\mathbf{y}}_n[1]$ is largest. That is we want to pick the direction $\mathbf{w}_1$ that maximize the sample variance in the projected direction which is given by:

$$\frac{1}{n}\sum_{t=1}^{n}\left(\hat{\mathbf{y}}_t[1] - \frac{1}{n}\sum_{t=1}^{n}\hat{\mathbf{y}}_t[1]\right)^2$$

Before we proceed it is useful to note that from Eq. 1, $\mathbf{x}_t - \boldsymbol{\mu} = \sum_{j=1}^{d}\mathbf{y}_t[j]\mathbf{w}_j$ and so taking dot product with any $\mathbf{w}_i$ we have,

$$\mathbf{w}_i^\top(\mathbf{x}_t - \boldsymbol{\mu}) = \mathbf{w}_i^\top\left(\sum_{j=1}^{d}\mathbf{y}_t[j]\mathbf{w}_j\right) = \sum_{j=1}^{d}\mathbf{y}_t[j]\mathbf{w}_i^\top\mathbf{w}_j$$

However since $\mathbf{w}$'s are orthonormal, $\mathbf{w}_i^\top\mathbf{w}_i = 1$ and $\mathbf{w}_i^\top\mathbf{w}_j = 0$ and so,

$$\mathbf{w}_i^\top(\mathbf{x}_t - \boldsymbol{\mu}) = \mathbf{y}_t[i] \tag{3}$$

Thus $\hat{\mathbf{y}}_t[1] = \mathbf{w}_1^\top(\mathbf{x}_t - \boldsymbol{\mu})$. Hence the solution for $\mathbf{w}_1$ is given by:

$$\begin{aligned}\mathbf{w}_1 &= \arg\max_{\mathbf{w}:\|\mathbf{w}\|_2^2=1}\frac{1}{n}\sum_{t=1}^{n}\left(\mathbf{w}^\top(\mathbf{x}_t - \boldsymbol{\mu}) - \frac{1}{n}\sum_{t=1}^{n}\mathbf{w}^\top(\mathbf{x}_t - \boldsymbol{\mu})\right)^2 \\ &= \arg\max_{\mathbf{w}:\|\mathbf{w}\|_2^2=1}\frac{1}{n}\sum_{t=1}^{n}\left(\mathbf{w}^\top\mathbf{x}_t - \frac{1}{n}\sum_{t=1}^{n}\mathbf{w}^\top\mathbf{x}_t\right)^2\end{aligned}$$

Now let us simplify the above expression further,

$$\begin{aligned}
\mathbf{w}_1 &= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \frac{1}{n}\sum_{t=1}^{n}\left(\mathbf{w}^\top \mathbf{x}_t - \frac{1}{n}\sum_{t=1}^{n}\mathbf{w}^\top \mathbf{x}_t\right)^2 \\
&= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \frac{1}{n}\sum_{t=1}^{n}\left(\mathbf{w}^\top \left(\mathbf{x}_t - \frac{1}{n}\sum_{t=1}^{n}\mathbf{x}_t\right)\right)^2 \\
&= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \frac{1}{n}\sum_{t=1}^{n}\left(\mathbf{w}^\top (\mathbf{x}_t - \mu)\right)^2 \\
&= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \frac{1}{n}\sum_{t=1}^{n}\mathbf{w}^\top (\mathbf{x}_t - \mu)(\mathbf{x}_t - \mu)^\top \mathbf{w} \\
&= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \mathbf{w}^\top \left(\frac{1}{n}\sum_{t=1}^{n}(\mathbf{x}_t - \mu)(\mathbf{x}_t - \mu)^\top\right)\mathbf{w} \\
&= \arg \max_{\mathbf{w}:\|\mathbf{w}\|_2=1} \mathbf{w}^\top \Sigma \mathbf{w}
\end{aligned}$$

Where Σ is sample the covariance matrix.

The first direction we pick will be the the unit vector $\mathbf{w}_1$ that maximizes $\mathbf{w}_1^\top \Sigma \mathbf{w}_1$

(Roughly speaking) Whenever we want to maximize (or minimize) a function subject to a constraint, we can use the idea of Lagrange multipliers. What the result says is that there exists $\lambda_1 \in \mathbb{R}$ such that the solution to $\mathbf{w}_1$ can be alternatively written down as :

$$\mathbf{w}_1 = \arg \max_{\mathbf{w}\in\mathbb{R}^d} \mathbf{w}^\top \Sigma \mathbf{w} - \lambda \|\mathbf{w}\|_2^2$$

To optimize the above we simply take derivative and equate to 0. This gives us

$$\Sigma \mathbf{w}_1 - \lambda \mathbf{w}_1 = 0$$

The direction $\mathbf{w}_1$ we obtain by maximizing the variance in the direction is some unit vector that satisfies

$$\Sigma \mathbf{w}_1 = \lambda \mathbf{w}_1$$

But this is exactly the definition of an eigen vector of matrix Σ. In Dutch the word "eigen" means self or own. Eigen vector of a matrix multiplied to the matrix results in a vector that is the just a scaled version of the eigenvector itself.

So we see that $\mathbf{w}_1$ is an eigenvector of Σ. The next question is, which eigen vector to choose. To this end note that we want to maximize $\mathbf{w}_1^\top \Sigma \mathbf{w}_1$ and we just saw that $\Sigma \mathbf{w}_1 = \lambda \mathbf{w}_1$. Hence

$$\mathbf{w}_1^\top \Sigma \mathbf{w}_1 = \lambda \|\mathbf{w}_1\|_2^2 = \lambda$$

Since we want to maximize the above quantity it stands to reason that we pick $\mathbf{w}_1$ to be the eigen vector corresponding to the largest eigen value of Σ. For $\mathbf{w}_2, \ldots, \mathbf{w}_K$ we proceed in similar fashion and pick the eigen vectors that have the second largest, up to the Kth largest eigen values.

4 View II: Minimizing Reconstruction Error

Basic idea: Another way of thinking about which orthonormal basis to choose is to pick the basis such that the reconstruction error is minimized. That is pick the orthonormal basis $\mathbf{w}_1, \ldots, \mathbf{w}_K$ such that

$$\frac{1}{n}\sum_{t=1}^{n} \|\mathbf{x}_t - \hat{\mathbf{x}}_t\|_2^2$$

is minimized. (See the figure on page 2).

Let us simplify the above term,

$$\begin{aligned}
\frac{1}{n}\sum_{t=1}^{n} \|\hat{\mathbf{x}}_t - \mathbf{x}_t\|_2^2 &= \frac{1}{n}\sum_{t=1}^{n} \left\| \sum_{j=1}^{K} \mathbf{y}_t[j]\mathbf{w}_j + \mu - \mathbf{x}_t \right\|_2^2 \\
&= \frac{1}{n}\sum_{t=1}^{n} \left\| \sum_{j=1}^{K} \mathbf{y}_t[j]\mathbf{w}_j + \mu - \sum_{j=1}^{d} \mathbf{y}_t[j]\mathbf{w}_j - \mu \right\|_2^2 \\
&= \frac{1}{n}\sum_{t=1}^{n} \left\| \sum_{j=K+1}^{d} \mathbf{y}_t[j]\mathbf{w}_j \right\|_2^2 \qquad \text{(note that } \mathbf{y}_t[j] = \mathbf{w}_j^\top(\mathbf{x}_t - \mu) \text{ from Eq. 3)} \\
&= \frac{1}{n}\sum_{t=1}^{n} \left\| \sum_{j=K+1}^{d} (\mathbf{w}_j^\top(\mathbf{x}_t - \mu))\mathbf{w}_j \right\|_2^2
\end{aligned}$$

from the above to the next equation is not hard but just takes a bit of staring. Note that for any vector $\mathbf{v}$, $\|\mathbf{v}\|_2^2 = \mathbf{v}^\top\mathbf{v}$. Expanding the above and noticing that $\mathbf{w}_j$'s are orthonormal yields the below. It's ok if this step seems hard, just take it as given.

$$\begin{aligned}
&= \frac{1}{n}\sum_{t=1}^{n}\sum_{j=K+1}^{d} \left(\mathbf{w}_j^\top(\mathbf{x}_t - \mu)\right)^2 \\
&= \frac{1}{n}\sum_{t=1}^{n}\sum_{j=K+1}^{d} \mathbf{w}_j^\top(\mathbf{x}_t - \mu)(\mathbf{x}_t - \mu)^\top\mathbf{w}_j \\
&= \sum_{j=K+1}^{d} \mathbf{w}_j^\top \left(\frac{1}{n}\sum_{t=1}^{n}(\mathbf{x}_t - \mu)(\mathbf{x}_t - \mu)^\top\right)\mathbf{w}_j \\
&= \sum_{j=K+1}^{d} \mathbf{w}_j^\top \Sigma \mathbf{w}_j
\end{aligned}$$

The orthonormal basis $\mathbf{w}_1, \ldots, \mathbf{w}_d$ that we shall pick are the ones that minimize the reconstruction error and are hence the orthonormal basis that minimize, $\sum_{j=K+1}^{d} \mathbf{w}_j^\top \Sigma \mathbf{w}_j$.

We again use the Lagrangian multipliers to rewrite the constrained minimization problem (with the unit norm constraints) into an unconstrained minimization problem. Specifically we see that

there exists $\lambda_1, \ldots, \lambda_d$ such that the orthonormal basis $\mathbf{w}_1, \ldots, \mathbf{w}_d$ are the ones that minimize,

$$\sum_{j=K+1}^{d} \mathbf{w}_j^\top \Sigma \mathbf{w}_j - \sum_{j=1}^{d} \lambda_j \|\mathbf{w}_j\|_2^2$$

Taking derivative and equating to 0 we find that for any index $K+1 \leq j \leq d$,

$$\Sigma \mathbf{w}_j - \lambda_j \mathbf{w}_j = 0$$

Thus again we find that the $\mathbf{w}$'s are eigen vectors.

To minimize the reconstruction error we simply pick the eigen basis of Σ and retain K of them while throwing away the remaining. Now since each $\mathbf{w}_j$ is an eigen vector we have that

$$\Sigma \mathbf{w}_j = \lambda_j \mathbf{w}_j$$

where λ_j is the corresponding eigen value. Now the question remains, which Eigen vector to keep and which to throw away. To this end recall that we want to minimize

$$\sum_{j=K+1}^{d} \mathbf{w}_j^\top \Sigma \mathbf{w}_j = \sum_{j=K+1}^{d} \lambda_j \mathbf{w}_j^\top \mathbf{w}_j = \sum_{j=K+1}^{d} \lambda_j$$

Thus it stands to reason that to minimize the above we pick $\mathbf{w}_{K+1}, \ldots, \mathbf{w}_d$ to be the eigenvectors with the $d-K$ smallest eigenvalues. **That is we throw away the bottom $d-K$ eigen vectors and only retain the top K of them.**

5 PCA Algorithm

What both the views tell us is that the matrix W we shall use for PCA is got by taking the K eigenvectors corresponding to the top K eigen values. As for the PCA algorithm, one way to implement it is to first compute the covariance matrix given the data. This can be done by calculating the mean vector and then covariance matrix as

$$\boldsymbol{\mu} = \frac{1}{n} \sum_{t=1}^{n} \mathbf{x}_t \qquad \Sigma = \frac{1}{n} \sum_{t=1}^{n} (\mathbf{x}_t - \boldsymbol{\mu})(\mathbf{x}_t - \boldsymbol{\mu})^\top = \frac{1}{n} (X - \mu)^\top (X - \mu)$$

Next we perform eigen decomposition of the matrix and take the top K eigen vectors and set

$$W = \left[\mathbf{w}_1, \ldots, \mathbf{w}_K^\top \right]$$

5.1 Projection to Lower Dimension

Projection is simply given by

$$\mathbf{y}_t = (\mathbf{x}_t - \boldsymbol{\mu})^\top W$$

5.2 Reconstruction

Reconstruction of the data points based on low dimensional representation is given by

$$\hat{\mathbf{x}}_t = \mathbf{y}_t^\top W^\top + \boldsymbol{\mu}$$