Math 690: Topics in Data Analysis and Computation
Lecture notes for August 31, 2017

Scribed by Yixin Lin

We ended last time on a few basics of machine learning.

An important point is to be careful not to "cheat" when measuring the performance of your models! Of course you want to know how well your model works on your current dataset, but you can fail on datasets that you haven't seen before. This is the concept of **generalization**: we want our models to generalize to the unseen samples as well.

Machine learning basics

Goal: $y = f^*(x)$.

$$x_i \sim P_x, \text{ iid}, \quad y_i = f^*(x_i)$$

Training set $D_{Tr} = \{x_i, y_i\}_{i=1}^{n_{Tr}}$

Testing set (independent of training set, but from the same distribution) $D_{Te} = \{x_j, y_j\}_{j=1}^{n_{Te}}$

Training error: error on the training dataset.

Test error: error using trained model on test set. (also known as generalization error)

Recall that test error is

$$\varepsilon_{Te}(\theta) = \frac{1}{n_{Te}} \sum_{j=1}^{n_{Te}} (y_j - f_\theta(x_j))^2 \to^{n\to\infty} \int (f^*(x) - f_\theta(x))^2 p(x) dx$$

We are trying to search for parameters $\theta \in \Theta$ such that $f_\theta(x) \approx f^*(x)$.

The issues of overfitting and under-fitting: f^* may not be in the family we are considering. When the family is too small, the trained model underfits. Thus we want to enlarge our family of models. However, we may need more samples to estimate f^* when considering a large family. If we don't have enough samples, the trained model overfits and poorly generalizes to unobserved samples.

Breakdown of error

We can break down the error into three terms: the approximation error, estimation error, and optimization error. ([ref] This is Part I of "The Tradeoffs of Large-scale Learning" by Leon Botton, 2007.)

Our true objective is minimizing the error

$$\varepsilon(\theta) = \int (f^*(x) - f_\theta(x))^2 dp(x) = \mathbb{E}_{x\sim p} |y - f_\theta(x)|^2$$

but we know that our family of models may not be big enough. As long as f^* is not in the family of functions we are considering, then this error will never be zero:

$$\min_{\theta\in\Theta} \varepsilon(\theta) = \varepsilon(\theta^*) > 0$$

Even if you have infinite training samples, if your family is small, then the error *will never go to zero.* We call this the **bias** term.

We don't know p, so we don't know how to compute the integral. So what we really do in practice is minimize the training error. Instead of $\min_\theta \varepsilon(\theta)$, we minimize the following:

$$\hat{\theta} = \arg\min_{\theta\in\Theta} \hat{\varepsilon}(\theta) = \frac{1}{n}\sum_{i=1}^{n}(y_i - f_\theta(x_i))^2$$

which is a finite sample approximation of the integral, and in general $\hat{\theta} \neq \theta^*$. This means that $\varepsilon(\hat{\theta}) > \varepsilon(\theta^*)$.

Let us write $\varepsilon(\hat{\theta}) = \varepsilon(\theta^*) + (\varepsilon(\hat{\theta}) - \varepsilon(\theta^*))$. $(\varepsilon(\hat{\theta}) - \varepsilon(\theta^*))$ is the **estimation error**.

The third term of optimization will be that we want to minimize our previous error, but we are using a computer to approximate and compute this. The third term of the breakdown is **optimization error** and caused by imperfection in the optimization of

$$\arg\min_{\theta\in\Theta} \hat{\varepsilon}(\theta)$$

This imperfection causes there to be an additional term:

$$\Rightarrow \varepsilon(\theta_{\text{sol}}) = \varepsilon(\hat{\theta}) + \varepsilon_{\text{opt}}$$

$$\varepsilon = \varepsilon_{\text{approx}} + \varepsilon_{\text{est}} + \varepsilon_{\text{opt}}$$

We mainly first focus on the first two terms in this class.

No free lunch theorem

[ref] "The Lack of A Priori Distinctions Between Learning Algorithms" Wolpert '96.

The question is, do we have a model better than another? No machine learning model is uniformly better than another.

What do we mean by *better*?

No free lunch theorem for optimization

Our goal is to minimize some function $f : V \to S$. For any two models A and B, the *averaged* performance of A and B are identical.

What do we mean by averaged performance? Over $\sum_f$, f is uniformly averaged over S^V.

No free lunch theorem for machine learning

For any two models A and B, there are "as many" targets for which model A has lower generalization error than model B, and vice versa. In other words, I can always find some dataset for A to work worse than B, and vice versa. So we need more assumptions about the distribution of the data.

The take-home message is that for the question of "which algorithm is better", the answer is *it depends on the data.*

Topic 1: Principal Component Analysis in High Dimension

Two perspectives: the linear algebra perspective, and the probability perspective

Linear algebra perspective

Suppose I have data vectors

$$x_1, \cdots, x_n \in \mathbb{R}^D$$

with center of mass in the origin: $\sum_{i=1}^n x_i = 0$. (Here, $D = p$, the dimensionality of the data.)

Our goal is to find the "optimal" d-subspace to maximize the projected variation of data. (Maximizing variation is minimizing residual; verifying this is a homework problem.)

Let $d = 1$, $w \in \mathbb{R}^p$, and constrain $\|w\| = 1$.

$$\max_w \sum_{i=1}^n (w^T w_i)^2 = \sum_{i=1}^n w^T x_i x_i^T w$$

$$= w^T (\sum_{i=1}^n x_i x_i^T) w$$

$$S \triangleq \frac{1}{n} \sum_{i=1}^n x_i x_i^T$$

So our goal is

$$\max_w w^T S w \text{ s.t. } \|w\| = 1$$

We need to also add the constraint that $w_k^T w_k = 1$, $w_k^T w_l = 0$ for all $k \neq l$. Equivalently, $w_k^T w_l = \delta_{kl}$. In other words, the vectors should be mutually orthogonal.

Objective will be

$$\max_{w_1, \cdots, w_d} \sum_{k=1}^d w_k^T S w_k$$

with the constraint of orthogonality.

We know the solution to this problem from linear algebra: the first d eigenvectors of S.

S has p non-negative eigenvalues $\lambda_1, \cdots, \lambda_p$ (sorted by magnitude $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p$) associated with p eigenvectors $v_1, \cdots, v_p$.

To solve this problem, compute the eigendecomposition of the covariance matrix can be computed by the singular value decomposition (SVD) of X.

So far there is no probability.

Probability perspective

Suppose $\{x_i\}_{i=1}^n \sim^{\text{i.i.d.}} P$, in $\mathbb{R}^p$.

$$\mathbb{E} x_i = 0, \mathbb{E} x_i x_i^T = \Sigma_{p \times p}$$

Our goal:

$$\max_{w_1, \cdots, w_d | w_k^T w_l = \delta_{kl}} \sum_{k=1}^d \mathbb{E}_{x \sim P} (x^T w_k)^2$$

where the notation $\mathbb{E}_{x \sim p} f(x) = \int f(x) dP(x)$, we interchange $dP(x)$ with $p(x)dx$, $p(x)$ being the probability density. The objective is thus

$$\sum_{k=1}^{d} w_k^T (\mathbb{E}_{x\sim p} x x^T) w_k = \sum_{k=1}^{d} w_k^T \Sigma w_k.$$

The solution is obtained by the eigendecomposition of Σ.

However, the population covariance matrix Σ is usually not available, and we approximate it by the sample covariance S, which goes back to the PCA of finite samples (the 1st perspective).