Data mining

Giacomo Fantoni
Telegram: @GiacomoFantoni
Github: https://github.com/giacThePhantom/DataMining

December 14, 2021

Contents

Chapter 1

Introduction

A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T as measured by P, improves with experience E.
From that it is understood that machine learning is a form of inductive learning: it generalize from examples to a concept. There is no certainty of correctness.

1.1 Formalization of a machine learning problem

1.1.1 Components of a machine learning problem

The components of a machine learning problem are:

- Task to be addressed by the system.
- Performance measure to evaluate the learned system.
- Training experience to train the learning system.

1.1.2 Designing a machine learning system

The designing of a machine learning system can be described in a process that consist of different phases:

1. Formalize the learning task.
2. Collect data.
3. Extract features.
4. Choose class of learning models.
5. Train model.
6. Evaluate model.

1.1.2.1 Formalize the learning task

To formalize the learning task means to define the task that should be addressed by learning system. This type of task, or learning problem, is often composed of a number of related tasks, sub-problems or side-tasks. It is also needed an appropriate performance measure for evaluating the learned system.

1.1.2.2 Collect data

To collect the data means to collect a set of training example in machine readable format. Data collection is often the most cumbersome part of the process, implying manual intervention especially in labelling examples for supervised learning. Recent approaches to the problem of data labelling try to make use of the availability of unlabelled data (semi-supervised learning it tries to learn using both supervised and unsupervised examples).

1.1.2.3 Extract features

A relevant set of features need to be extracted from the data in order to provide inputs to the learning system. Prior knowledge is usually necessary in order to choose the appropriate features for the task in mind. Extracting too few features can miss relevant information preventing the system from learning the task with reasonable performance. Extracting too many feature like can make the learning problem harder and require a number of examples greater than those available for training. Another problem arises when considering noisy features. It is noticeable that there is a need to choose the correct number and type of feature to permit a correct and efficient solution.

1.1.2.4 Choose class of learning models

Every problem has a class of learning model that is able to learn it best. A simple model like a linear classifier is easy to train but insufficient for non linearly separable data. A too complex model can memorize noise in training data failing to generalize to new examples. The algorithm need not to optimize but it needs to generalize, there can be outliers or labelling error. The more complex the model the more it will tend to overfit training noise.

1.1.2.5 Train model

Training a model implies searching though the space of possible models given the chosen model class. Such search typically aims at fitting the available training examples well according to the chosen performance measure. However the learned model should perform well on unseen data (generalization) and not simply memorize training examples (overfitting). Different techniques can be used to improve generalization, usually by trading off model complexity with training set fitting.

1.1.2.6 Evaluate model

The learned model is evaluated according to its ability to generalize to unseen examples. These example are collected in a test set. Evaluation can provide insights into the model weaknesses and suggest directions for refining and modifying it. Evaluation can imply comparing different models or learners in order to decide the best performing one. Statistical significance of observed differences between performance of different models should be assessed with appropriate statistical tests.

1.2 Learning settings

1.2.1 Supervised learning

The learner is provided with a set of inputs/output pairs $(x_i, y_i) \in X \times Y$. The learned model $f : x \to Y$ should map input examples into their output. A domain expert is typically involved in labelling input examples with output examples in the training set.

1.2.1.1 Tasks

1.2.1.1.1 Classification

- Binary: assign an example to one of two possible classes often a positive and a negative one.
- Multiclass: assign an example to one of $n > 2$ possible classes.
- Multilabel: assign an example to a subset $m \leq n$ of the possible classes.

1.2.1.1.2 Regression Assign a real value to an example.

1.2.1.1.3 Ordinal regression or ranking Order a set of examples according to their relative importance or quality with respect to the class.

1.2.2 Unsupervised learning

The learner is provided a set of input examples $x_i \in X$ with no labelling information. The learner models training examples, for examples clustering them together into clusters according to their similarity.

1.2.2.1 Tasks

1.2.2.1.1 Dimensionality reduction Reduce dimensionality of the data maintaining as much information as possible.

1.2.2.1.2 Clustering Cluster data into homogeneous groups according to their similarity.

1.2.2.1.3 Novelty detection Detect novel examples which differ from the distribution of a certain set of data.

1.2.3 Semi-supervised learning

The learner is provided with a set of input output pairs $(x_i, y_i) \in X \times Y$. A typically much bigger additional set of unlabelled examples $x_i \in X$ is also provided. Like in supervised learning the learned model $f : X \to Y$ should map input examples into their output. Unlabelled data can be exploited to improve performance, by forcing the model to produce similar outputs for similar inputs, or by allowing to learn a better representation of examples.

1.2.4 Reinforcement learning

The learner is provided a set of possible states S and for each state a set of possible actions A moving it to a next state. In performing action a from state s the learner is provided an immediate reward $r(s, a)$. The task is to learn a policy allowing to choose for each state s the action a maximizing the overall reward. The learner has to deal with problems of delayed reward coming from future moves and trade-off between exploitation and exploration. Typical application include moving policies for robots and sequential scheduling problems in general.

1.3 Probabilistic reasoning

Probabilistic reasoning is the reasoning in presence of uncertainty. It evaluates the effect of a certain piece of evidence on other related variables. It estimates probabilities and relations between variables from a set of informations. They depends on variables and their relations.

1.4 Choice of learning algorithms

1.4.1 Based on information available

- Full knowledge of probability distributions of data: Bayesian decision theory.
- Form of probabilities known, parameters unknown: parameter estimation from training data.
- Form of probabilities unknown, training examples available: discriminative methods: do not model input data, learn a function predicting the desired output given the input.
- Form of probabilities unknown, training examples unavailable: unsupervised methods, cluster examples by similarity.

Chapter 2

Decision trees learning

2.1 Introduction

Decision trees tend to be interpretable, it is easy to see the reason for a certain decision. They represent a disjunction of conjunctions of constraints over attribute values. Each path from the root to a leaf is a conjunction of the constraints specified in the nodes along it: they can be seen as a disjunctive normal formula. In this way every class can be written as a DNF. The leaf contains the label to be assigned to instances reaching it. The disjunction of all paths is the logical formala expressed by the tree.

2.1.1 Appropriate problems for decision trees

The class of problems that can be solved by decision trees are:

- Binary or multiclass classification with an extension to regression (with a linear regression as the leaf).
- Instances represented as attribute-value pairs.
- Different explanations for the concept are possible (disjunction).
- Some instances have missing attributes, its dealing done with probabilistic models.
- There is need for an interpretable explanation of the output. In fact the main reason for using decision tress is interpretability.

2.2 Learning decision trees

2.2.1 Greedy top-down strategy

For each node, starting from the root with full training set:

1. Choose best attribute to be evaluated.
2. Add a child for each attribute value.
3. Split node training set into children according to value of chosen attribute.

4. Stop splitting a node if it contains examples from a single class or there are no more attributes to test.

It is also known as the divide et impera approach.

2.2.2 Choosing the best attribute

A measure to choose the attribute is entropy. It measures the amount of information contained in a collection of instances S which can take a number c of possible values:

$$H(s) = -\sum_{i=1}^{c} p_i \log_2 p_i$$

Where p_i is the fraction of S taking value i. In our case instances are training examples and values are class labels. The entropy of a set of labelled examples measures its label's inhomogeneity.

2.2.2.1 Information gain

Expected reduction in entropy obtained by partitioning a set S according to the value of a certain attribute A.

$$IG(S, A) = H(S) - \sum_{v \in Values(A)} \frac{|S_v|}{|S|} H(S_V)$$

Where $Values(A)$ is the set of possible values taken by A and S_v is the subset of S taking value v at attribute A. The second term represents the sum of entropies of subsets of examples obtained partitioning over A values, weighted by their respective sizes. An attribute with high information gain tends to produce homogeneous groups in terms of labels, thus favouring their classification. The idea is to use the greedy strategy in which at each choice it is chosen the attribute with the maximum information gain.

2.3 Issues in decision tree learning

2.3.1 Overfitting avoidance

Requiring that each leaf has only examples of a certain class can lead to very complex trees. A complex tree can easily overfit the training set, incorporating random regularities not representative of the full distribution, or noise in the data. It is possible to accept impure leaves, assigning them the label of the majority of their training examples. Two possible strategies to prune a decision tree are:

- Pre-pruning; decide whether to stop splitting a node even if it contains training examples with different labels.
- Post-pruning: learn a full tree and then prune it.

2.3.2 Post-pruning

In post-pruning you expand the tree and then you prune it. It is introduced the validation set.

1. For each node in the tree evaluate the performance on the validation set when removing the subtree rooted at it.

2. If all node removals worsen performance, stop.
3. Choose the node whose removal has the best performance inprovement.
4. Replace the subtree rooted at it with a leaf.
5. Assign to the leaf the majority label of all examples in the subtree.
6. Return to 1.

2.3.3 Dealing with continues valued attributes

Continuous valued attributes need to be discretized in order to be used in internal node tests. Discretization threshold can be chosen in order to maximize the attribute quality criterion.

1. Examples are sorted according to their continuous attribute values.
2. For each pair of successive examples having different labels, a candidate threshold is placed as the average of the two attribute values.
3. For each candidate threshold the infogain achieved splitting examples according to it is computed.
4. The threshold producing the higher infogain is used to discretize the attribute.

2.3.4 Alternative attribute test measures

The information gain criterion tends to prefer attributes with a large number of possible values. As an extreme the unique ID of each examples is an attribute perfectly splitting the data into singletons, but it will be no use on new examples. A measure of such spread is the entropy of the dataset with respect to the attribute value instead of the class value:

$$H_A(S) = -\sum_{v \in Values(A)} \frac{|S_V|}{|S|} \log_2 \frac{|S_V|}{|S|}$$

The gain ration measures downweights the information gain by such attribute value entropy:

$$IGR(S, A) = \frac{IG(S, A)}{H_A(S)}$$

2.3.5 Handling attributes with missing values

Assume example x with class $c(x)$ has missing value for attribute A. When attribute A is to be tested at node n:

- Simple solution: Assign to x the most common attribute values among examples in n or the most common of examples in n with class $c(x)$.
- Complex solution: Propagate x to each of the children of n with a fractional value equal to the proportion of examples with the corresponding attribute value.

The complex solution implies that at test time, for each candidate class, all fractions of the test example which reached a leaf with that class are summed, and the example is assigned the class with highest overall value.

2.4 Random forest

Random forests are an ensemble of decision trees. An ensemble is a method by which predictions are given by a set of predictors and is taken the prediction most represented. They improve stability and accuracy of the predictions. Random forests are effective and one of the methods of choice in case of tabular data.

2.4.1 Training

To train a random forest:

1. Given a training set of N examples, sample N examples with replacement.
2. Train a decision tree on the sample, selecting at each node m features at random among which to choose the best one.
3. Repeat the first two step M times in order to generate a forest of M trees.

2.4.2 Testing

To test a random forest:

1. Test the example with each tree in the forest.
2. Return the majority class among the predictions.

Chapter 3

K-nearest neighbours

3.1 Introduction

The K-nearest neighbours is an algorithm that, given a training set represented as a vector of features, gives the label for a new sample as label of the majority of the K nearest sample in the training set.

3.2 Measuring the instance between instances

3.2.1 Metric or distance definition

Given a set $\mathcal{X}$ a function $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_0^+$ is a metric for $\mathcal{X}$ if for any $x, y, z \in \mathcal{X}$ the following properties are satisfied:

- Reflexivity $d(x, y) = 0 \Leftrightarrow x = y$.
- Symmetry $d(x, y) = d(y, x)$.
- Triangle inequality $d(x, y) + d(y, z) \geq d(x, z)$.

3.2.2 Euclidean distance

The euclidean distance in $\mathbb{R}^n$ is:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

3.3 Algorithms

3.3.1 Classification

: `Knn-Classification()`

foreach *test examples* x **do**
  foreach *training examples* (x_i, y_i) **do**
    compute distance $d(x, x_i)$
  select k-nearest neighbours of x
  %`return class of` x `as majority class among neighbours`
  return $\arg\max_{x_y} \sum_{i=1}^{k} \delta(y, y_i)$

3.3.2 Regression

: `Knn-Regression()`

foreach *test examples* x **do**
  foreach *training examples* (x_i, y_i) **do**
    compute distance $d(x, x_i)$
  select k-nearest neighbours of x
  %`return the average output value among neighbours`
  return $\frac{1}{k} \sum_{i=1}^{k} y_i$

3.4 Characteristics

- Instance-based learning: the model used for prediction is calibrated for the test example to be processed.
- Lazy learning: the computation is mostly deferred to the classification phase.
- Local learner: assumes prediction should mainly influenced by nearby instances.
- Uniform feature weighting: all feature are uniformly weighted in computing dinstances.

3.5 Distance weighted k-nearest neighbour

The distance weighted k-nearest neighbour is a variant of the classic k-nearest neighbour in which the distance is weighted. The weight of a point is calculated as:

$$w_i = \frac{1}{d(x, x_i)}$$

The class is decided for classification according to the formula:

$$\arg\max_{x_y} \sum_{i=1}^{k} w_i \delta(y, y_i)$$

For regression the formula is instead:

$$\frac{\sum_{i=1}^{k} w_i y_i}{\sum_{i=1}^{k} w_i}$$

Chapter 4

Linear algebra

4.1 Vector space

A set $\mathcal{X}$ is called a vector space over $\mathbb{R}$ if addition and scalar multiplication are defined and satisfy for all $x, y, z \in \mathcal{X}$ and $\lambda, \mu \in \mathcal{R}$:

- Addition:
  - Association: $x + (y + z) = (x + y) + z$.
  - Commutation: $x + y = y + x$.
  - There is an identity element: $\exists 0 \in \mathcal{X} : x + 0 = x$.
  - There is an inverse element: $\forall x \in \mathcal{X} \exists x' \in \mathcal{X} : x + x' = 0$.
- Scalar multiplication:
  - Is distributive over elements: $\lambda(x + y) = \lambda x + \lambda y$.
  - Is distributive over scalars: $(\lambda + \mu)x = \lambda x + \mu x$.
  - Is associative over scalars: $\lambda(\mu x) = (\lambda\mu)x$.
  - There is an identity element: $\exists 1 \in \mathbb{R} : 1x = x$.

4.1.1 Properties and operations

4.1.1.1 Subspace

A subspace is any non-empty subset of $\mathcal{X}$ being itself a vector space.

4.1.1.2 Linear combination

Given $\lambda_i \in \mathbb{R} \wedge x_i \in \mathcal{X}$, a linear combination is:

$$\sum_{i=1}^{n} \lambda_i x_i$$

4.1.1.3 Span

The span of vectors $x_1, \ldots, x_n$ is defined as the set of their linear combination:

$$\{\sum_{i=1}^{n} \lambda_i x_i, \lambda_i \in \mathbb{R}\}$$

4.1.1.4 Linear independence

A set of vector x_i is linearly independent if none of them can be written as a linear combination of the others.

4.1.2 Basis

A set of vectors x_i is a basis for $\mathcal{X}$ if any element in $\mathcal{X}$ can be uniquely written as a linear combination of vectors x_j. The vectors x_j need to be linearly independent. All bases of $\mathcal{X}$ have the same number of elements, called the dimension of the vector space.

4.2 Matrices

4.2.1 Linear maps

Given two vector spaces $\mathcal{X}$ and $\mathcal{Z}$ a function $f : \mathcal{X} \to \mathcal{Z}$ is a linear map if $\forall x, y \in \mathcal{X} \lambda \in \mathbb{R}$:

- $f(x + y) = f(x) + f(y)$.
- $f(\lambda x) = \lambda f(x)$.

4.2.2 Linear maps as matrices

A linear map between two finite dimensional spaces $\mathcal{X}$ and $\mathcal{Z}$ of dimension n and m can always be written as a matrix. Let $\{x_1, \ldots, x_n\}$ and $\{z_1, \ldots, z_m\}$ be some bases for $\mathcal{X}$ and $\mathcal{Z}$ respectively. For any $x \in \mathcal{X}$:

$$f(x) = f(\sum_{i=1}^{n} \lambda_i x_i) = \sum_{i=1}^{n} \lambda_i f(x_i)$$
$$f(x_i) = \sum_{j=1}^{m} a_{ji}^m a_{ij} z_j$$
$$f(x) = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_i a_{ji} z_j = \sum_{j=1}^{m}\big(\sum_{i=1}^{n} \lambda_i a_{ji}\big) z_j = \sum_{j=1}^{m} \mu_j z_j$$

4.2.2.1 Matrix of basis transformation

A matrix can be used to transform the basis is:

$$M \in \mathbb{R}^{m \times n} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

The mapping from basis to basis coefficient is done:

$$M\lambda = \mu$$

4.2.2.2 Matrix changing the coordinates, 2D examples

Let $B = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ be the standard basis in $\mathbb{R}^2$ and $B' = \left\{ \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ 1 \end{bmatrix} \right\}$ be an alternative basis. The change of coordinate matrix from B' to B is:

$$P = \begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}$$

So that:

$$[v]_B = P[v]_{B'} \qquad \wedge \qquad [v]_{B'} = P^{-1}[v]_B$$

For arbitrary B and B' P's columns must be the B' vectors written in terms of the B ones.

4.2.3 Matrix properties

4.2.3.1 Transpose

The transpose matrix is the matrix obtained exchanging the rows with column M^T.

$$(MN)^T = N^T M^T$$

4.2.3.2 Trace

The trace is the sum of the diagonal elements of a matrix:

$$tr(M) = \sum_{i=1}^{n} M_{ii}$$

4.2.3.3 Inverse

The inverse is the matrix which multiplied with the original matrix gives the identity:

$$MM^{-1} = I$$

4.2.3.4 Rank

The rank of an $n \times m$ matrix is the dimension of the space spanned by its columns.

4.2.4 Matrix derivatives

$$\begin{aligned}
\frac{\partial M_X}{\partial x} &= M \\
\frac{\partial y^T M x}{\partial x} &= M^T y \\
\frac{\partial x^T M x}{\partial x} &= (M^T + M)x \\
\frac{\partial x^T M x}{\partial x} &= 2Mx \qquad \text{if } M \text{ is symmetric} \\
\frac{\partial x^T x}{\partial x} &= 2x
\end{aligned}$$

Results are columns vectors. Transposing the matrix gives the row vectors.

4.2.5 Metric structure

4.2.5.1 Norm

A function $||\cdot|| : \mathcal{X} \to \mathbb{R}_0^+$ is a norm $\forall x, y \in \mathcal{X}, \lambda \in \mathbb{R}$:

- $||x + y|| \leq ||x|| + ||y||$
- $||\lambda x|| = |\lambda| ||x||$
- $||x|| > 0 if x \neq 0$

4.2.5.2 Metric

A norm defines a metric $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_0^+$:

$$d(x, y) = ||x - y||$$

Not every metric gives rise to a norm.

4.2.6 Dot product

A dot product $\langle \cdot, \cdot \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ is a symmetric bilinear form which is positive semi-definite:

$$\langle x, x \rangle \geq 0 \forall x \in \mathcal{X}$$

A positive definite dot product satisfies:

$$\langle x, x \rangle = 0 \Leftrightarrow x = 0$$

4.2.6.1 Norm

Any dot product defines a corresponding norm via:

$$||x|| = \sqrt{\langle x, x \rangle}$$

4.2.6.2 Properties

4.2.6.2.1 Angle The angle θ between two vectors is defined as:

$$\cos\theta = \frac{\langle x, z\rangle}{||x||||z||}$$

4.2.6.2.2 Orthogonal Two vectors are orthogonal if $\langle x, y\rangle = 0$.

4.2.6.2.3 Orthonormal A set of vectors $\{x_1, \ldots, x_n\}$ is orthonormal is

$$\langle x_i, x_j\rangle = \delta_{ij}$$

Where $\delta_{ij} = 1$ if $i = j$, 0 otherwise. If x and y are n-dimensional column vectors, their dot product is computed as:

$$\langle x, y\rangle = x^T y = \sum_{i=1}^{n} x_i y_i$$

4.3 Eigenvalues and eigenvectors

Given a $n \times n$ matrix M the real value λ and non zero vector x are eigenvalue and the corresponding eigenvector of M if:

$$Mx = \lambda x$$

4.3.1 Cardinality

An $n \times n$ matrix has n eigenvalues, but less than n distinct ones. The number of eigenvalues is the number of linear independent eigenvectors.

4.3.2 Singular matrices

A matrix is singular if it has a zero eigenvalue:

$$Mx = 0x = 0$$

A singular matrix has linearly dependent columns.

4.3.3 Symmetric matrices

Eigenvectors corresponding to distinct eigenvalues are orthogonal:

$$\begin{aligned}\lambda\langle x, z\rangle &= \langle Ax, z\rangle = \\ &= (Ax)^T z = && = x^T A^T z = \\ &= x^T Az = \\ &\langle x, Az\rangle = \\ &= \mu\langle x, z\rangle\end{aligned}$$

4.3.4 Eigen-decomposition

4.3.4.1 Raleigh quotient

$$Ax = \lambda x$$
$$\frac{x^T Ax}{x^T x} = \lambda \frac{x^T x}{x^T x} = \lambda$$

4.3.4.2 Finding eigenvector

To find the eigenvector you need to maximize the eigenvalue:

$$x = \max_v \frac{v^T Av}{v^T v}$$

After that you need to normalize it so the solution is invariant to rescaling:

$$x \leftarrow \frac{x}{||x||}$$

4.3.4.3 Deflating matrix

$$\bar{A} = A - \lambda x x^T$$

The deflation turns x into a zero eigenvalue eigenvector:

$$\bar{A}x = Ax - \lambda x x^T x$$
$$Ax - \lambda x = 0$$

Other eigenvalues are unchanged as eigenvectors with distinct eigenvalues are orthogonal because the matrix is symmetric:

$$\bar{A}z = Az - \lambda x x^T z$$
$$\bar{A}z = Az$$

4.3.4.4 Iterating

The maximization procedure is repeated on the deflated matrix until solution is zero. Minimization is iterated to get eigenvectors with negative eigenvalues. Eigenvectors with zero eigenvalues are obtained extending the obtained set to an orthonormal basis.

4.3.4.5 Eigen-decomposition

Let $V = [v_1 \dots v_n]$ be a matrix with orthonormal eigenvectors as columns. Let A be the diagonal matrix of corresponding eigenvalues. A square symmetric matrix can be diagonalizes as:

$$V^T AV = \Lambda$$

A diagonalized matrix is simpler to manage and has the same properties as the original one.

4.3.4.5.1 Proof

$$A[v_1 \dots v_n] = [v_1 \dots v_n \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$$

$$AV = V\Lambda$$
$$V^{-1}AV = V^{-1}V\Lambda$$
$$V^TAV = \Lambda$$

V is a unitary matrix with orthonormal columns for which $V^{-1} = V^T$.

4.3.4.6 Positive semi-definite matrix

An $n \times n$ symmetric matrix M is positive semi-definite if all its eigenvalues are non-negative. Positive semi-definite:

- $\Leftrightarrow \forall x \in \mathbb{R}^n : x^TMx \geq 0$
- $\Leftrightarrow \exists B : M = B^TB$

4.3.4.7 Scaling transformation in standard basis

Let $x_i = [1, 0]$ and $x_2 = [0, 1]$ the standard orthonormal basis in $\mathbb{R}^2$. Let $x = [x_1, x_2]$ am arbitrary vector in $\mathbb{R}^2$. A linear transformation is a scaling transformation if it only stretches x along its directions.

4.3.4.8 Scaling transformation in eigenbasis

Let A be a non-scaling transformation in $\mathbb{R}$. Let $\{v_1, v_2\}$ be an eigenbasis for A. By representing vectors in $\mathbb{R}^2$ in terms of the $\{v_1, v_2\}$ basis A becomes a scaling transformation.

4.4 Principal component analysis

Principal component analysis or PCA is a non-supervised machine learning technique that accomplishes dimensionality reduction. Let X be a data matrix with correlated coordinates. PCA is a linear transformation mapping data to a system of uncorrelated coordinates. It corresponds to fitting an ellipsoid to the data, whose axis are the coordinates of the new space.

4.4.1 Procedure

Given a dataset $X \in \mathbb{R}^{n \times d}$ in d dimension: Compute the mean of the data:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

Center the data into the origin:

$$X - \begin{bmatrix} \bar{x} \\ \dots \\ \bar{x} \end{bmatrix}$$

Compute the data covariance:

$$C = \frac{1}{n} X^T X$$

Compute the orthonormal eigen-decomposition of C:

$$V^T C V = A$$

Us it as the new coordinate system:

$$x' = V^{-1} x = V^T x$$

This method assumes linear correlation and Gaussian distribution.

4.4.2 Dimensionality reduction

Each eigenvalue corresponds to the amount of variance in that direction. Select only the k eigenvalues with largest eigenvalue for dimensionality reduction:

$$W = [v_1, \ldots, v_k]$$

$$x' = W^T x$$

Chapter 5

Probability theory

5.1 Discrete random variables

5.1.1 Probability mass function

Given a discrete random variable X taking values in $\mathcal{X} = \{v_1, \ldots, v_m\}$ its probability mass function $P : \mathcal{X} \to [0, 1]$ is defined as:

$$P(v_i) = Pr[X = v_i]$$

This function satisfies:

- $P(x) \geq 0$
- $\sum_{x \in \mathcal{X}} = 1$

5.1.2 Expected value

The expected value, mean or average of a random variable x is:

$$\mathbb{E}[x] = \mu = \sum_{x \in \mathcal{X}} xP(x) = \sum_{i=1}^{m} v_i P(v_i)$$

The expectation operator is linear:

$$\mathbb{E}[\lambda x + \lambda' y] = \lambda \mathbb{E}[x] + \lambda' \mathbb{E}[y]$$

5.1.3 Variance

The variance of a random variable is the moment of inertia of its probability mass function:

$$Var[x] = \sigma^2 = \mathbb{E}[(x - \mu)^2] = \sum_{x \in \mathcal{X}} (x - \mu)^2 P(x)$$

The standard deviation σ indicates the typical amount of deviation from the mean one should expect for a randomly drawn value for x.

5.1.4 Properties of mean and variance

5.1.4.1 Second moment

$$\mathbb{E}[x^2] = \sum_{x \in \mathcal{X}} x^2 P(x)$$

5.1.4.2 Variance in term of expectation

$$Var[x] = \mathbb{E}[x^2] - \mathbb{E}[x]^2$$

5.1.4.3 Variance and scalar multiplication

$$Var[\lambda x] = \lambda^2 Var[x]$$

5.1.4.4 Variance of uncorrelated variables

$$Var[x + y] = Var[x] + Var[y]$$

5.1.5 Probability distributions

5.1.5.1 Bernoulli distribution

The Bernoulli distribution indicates a variable for which there are two values: 1 for success and 0 for failure. Its parameter is p the probability of success. Its probability mass function:

$$P(x; p) = \begin{cases} p & if x = 1 \\ 1 - p & if x = 1 \end{cases}$$

- $\mathbb{E}[x] = p$
- $Var[x] = p(1 - p)$

5.1.5.1.1 Proof of mean

$$\begin{aligned} \mathbb{E}[x] &= \sum_{x \in \mathcal{X}} xP(x) \\ &= \sum_{x \in \{0;1\}} xP(x) \\ &= 0 \cdot (1 - p) + 1 \cdot p = p \end{aligned}$$

5.1.5.1.2 Proof of variance

$$\begin{aligned} Var[x] &= \sum_{x \in \mathcal{X}} (x - \mu)^2 P(x) \\ &= \sum_{x \in \{0;1\}} (x - \mu)^2 P(x) \\ &= (0 - p)^2 (1 - p) + (1 - p)^2 p \\ &= p^2 (1 - p) + (1 - p)(1 - p)p \\ &= (1 - p)(p^2 + p - p^2) \\ &= (1 - p)p \end{aligned}$$

5.1.5.2 Binomial distribution

The binomial distribution is the probability of a certain number of successes in n independent Bernoulli trials. Its parameters are p the probability of success and n the number of trials. Its probability mass function:

$$P(x; p, n) = \binom{n}{x} p^x (1 - p)^{n - x}$$

- $\mathbb{E}[x] = np$
- $Var[x] = np(1-p)$

5.1.6 Pairs of discrete random variables

5.1.6.1 Probability mass function

Given a pair of discrete random variables X and Y taking values $\mathcal{X} = \{v_1, \ldots, v_m\}$ and $\mathcal{Y} = \{w_1, \ldots, w_n\}$ the joint probability mass function is defined as:

$$P(v_i, w_j) = Pr[X = v_i, Y = w_j]$$

This satisfies:

- $P(x, y) \geq 0$
- $\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x, y) = 1$

5.1.6.2 Properties

5.1.6.2.1 Expected value

$$\mu_x = \mathbb{E}[x] = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} xP(x, y)$$

$$\mu_y = \mathbb{E}[y] = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} yP(x, y)$$

5.1.6.2.2 Variance

$$\sigma_x^2 = Var[(x - \mu_x)^2] = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} (x - \mu_x)^2 P(x, y)$$

$$\sigma_y^2 = Var[(y - \mu_y)^2] = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} (y - \mu_y)^2 P(x, y)$$

5.1.6.2.3 Covariance

$$\sigma_{xy} + \mathbb{E}[(x - \mu_x)(y - \mu_y)] = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} (x - \mu_x)(y - \mu_y) P(x, y)$$

5.1.6.2.4 Correlation coefficient

$$\rho = \frac{\sigma_{xy}}{\sigma_x \sigma_y}$$

5.1.6.3 Multinomial distribution

Given n samples of an event with m possible outcomes, the multinomial distribution models the probability of a certain distribution of outcomes. It has parameters $p_1, \ldots, p_m$ probabiliry of each outcome and n the number of samples. Its probability mass function assumes $\sum_{i=1}^{m} x_i = n$ and it is:

$$P(x_1, \ldots, x_m; p_1, \ldots, p_m, n) = \frac{n!}{\prod_{i=1}^{m} x_i!} \prod_{i=1}^{m} p_i^{x_i}$$

- $\mathbb{E}[x_i] = np)i$
- $Var[x_i] = np_i(1 - p_i)$
- $Cov[x_i, x_j] = -np_ip_j$

:

$$P(x_1, \ldots, x_m; p_1, \ldots, p_m, n) = \frac{n!}{\prod_{i=1}^{m} x_i!} \prod_{i=1}^{m} p_i^{x_i}$$

- $\mathbb{E}[x_i] = np)i$
- $Var[x_i] = np_i(1 - p_i)$
- $Cov[x_i, x_j] = -np_ip_j$

5.2 Conditionally probability

The conditional probability is the probability of x once y is observed:

$$P(x|y) = \frac{P(x, y)}{P(y)}$$

Variables X and Y are statistical independent if and only if:

$$P(x, y) = P(x)P(y)$$

This implies:

- $P(x|y) = P(x)$
- $P(y|x) = P(y)$

5.2.1 Basic rules

5.2.1.1 Law of total probability

The marginal distribution of a variable is obtained from a joint distribution summing over all possible values of the other variable:

- $P(x) = \sum_{y \in \mathcal{Y}} P(x, y)$
- $P(y) = \sum_{x \in \mathcal{X}} P(x, y)$

5.2.1.2 Product rule

Conditional probabiliry definition implies that:

$$P(x, y) = P(x|y)P(y) = P(y|x)P(x)$$

5.2.2 Bayes' rule

$$P(y|x) = \frac{P(x|y)P(y)}{P(x)}$$

This allows to invert statistical connection between effects x and cause y:

$$posterior = \frac{likelihood \times prior}{evidence}$$

The evidence can be obtained using the sum rule from likelihood and prior:

$$P(x) = \sum_y P(x, y) = \sum_y P(x|y)P(y)$$

5.3 Continuous random variables

5.3.1 Cumulative distribution function

To generalize the probability mass function to continuous domains it is considered the probability of intervals:

$$W = (a < X \leq b) \qquad A = (X \leq a) \qquad B = (X \leq b)$$

W and A are mutually exclusive, so:

$$P(B) = P(A) + P(W) \qquad P(W) = P(B) - P(A)$$

$F(q) = P(X \leq q)$ is the cumulative distribution function of X a monotonic function such that the probability of an interval is the difference:

$$P(a < X \leq b) = F(b) - F(a)$$

5.3.2 Probability density function

The derivative of the cumulative distribution function:

$$p(x) = \frac{d}{dx}F(x) \qquad F(q) = P(X \leq q) = \int_{-\infty}^{q} p(x)dx$$

So that it respect the properties:

- $p(x) \geq 0$
- $\int_{-\infty}^{\infty} p(x)dx = 1$

The probability density function of a value x can be greater than one provided the integral is one.

- $\mathbb{E}[x] = \mu = \int_{-\infty}^{\infty} xp(x)dx$
- $Var[x] = \sigma^2 = \int_{-\infty}^{\infty} (x-\mu)^2 p(x)dx$

Definitions and formulae for discrete random variables carry over to continuous random variables with sums replaced by integrals.

5.3.3 Probability distribution

5.3.3.1 Gaussian or normal distribution

The normal distribution is a bell-shaped curved with parameters μ mean and σ^2 variance. Its probability density function is:

$$p(x; \mu, \sigma) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Where:

- $\mathbb{E}[x] = \mu$
- $Var[x] = \sigma^2$

The standard normal distribution is $N(0,1)$. Every normal distribution can be transformed in a standard one:

$$z = \frac{x - \mu}{\sigma}$$

5.3.3.2 Beta distribution

The beta distribution is defined in the interval $[0,1]$ with parameters α and β. Its probability density function is:

$$p(x;\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

Where:

- $\mathbb{E}[x] = \frac{\alpha}{\alpha+\beta}$
- $Var[x] = \frac{\alpha\beta}{(\alpha+\beta+1)}$
- $\Gamma(x+1) = x\Gamma(x)$
- $\Gamma(1) = 1$

It models the posterior distribution of parameter p of a binomial distribution after observing $n-1$ independent events with probability p and $\beta - 1$ with probability $1-p$.

5.3.3.3 Multivariate normal distribution

The multivariate normal distribution is the normal distribution for d-dimensional vectorial data. Its parameter are $\vec{\mu}$ mean vector and Σ covariance matrix. Its probability density function:

$$p(\vec{x},\vec{\mu},\Sigma) = \frac{1}{(2\pi)^{\frac{d}{2}}|\Sigma|^{\frac{1}{2}}} e^{-\frac{1}{2}(\vec{x}-\vec{\mu})^T\Sigma^{-1}(\vec{x}-\vec{\mu})}$$

Where:

- $\mathbb{E}[\vec{x}] = \vec{\mu}$
- $Var[\vec{x}] = \Sigma$

The standard measure of instance to mean is the squared Mahalanobis distance"

$$r^2 = (\vec{x}-\vec{\mu})^T\Sigma^{-1}(\vec{x}-\vec{\mu})$$

5.3.3.4 Dirichlet distribution

The Dirichlet distribution is defines in $x \in [0,1]^m$, $\sum_{i=1}^{m} x_i = 1$ It has parameters $\vec{\alpha} = \alpha_1,\ldots,\alpha_m$. Its probability density function is:

$$p(x_1,\ldots,x_m;\vec{\alpha}) = \frac{\Gamma((\alpha_0)}{\prod_{i=1}^{m}\Gamma(\alpha_i)} \prod_{i=1}^{m} x_i^{a_i-1}$$

Where $\alpha_0 = \sum_{j=1}^{m} \alpha_j$. Also:

- $\mathbb{E}[x_i] = \frac{\alpha_i}{\alpha_0}$
- $Var[x_i] = \frac{\alpha_i(\alpha_0 - \alpha_i)}{\alpha_0^2(\alpha_0+1)}$
- $Cps[x_i, x_j] = \frac{-\alpha_i \alpha_j}{a_0^2(\alpha_0+1)}$

This distribution models the posterior distribution of parameters p of a multinomial distribution after observing $\alpha_i - 1$ times each mutually exclusive event.

5.4 Probability laws

5.4.1 Expectation of an average

Consider a sample of $X_1, \ldots, X_n$ instances drawn from a distribution with mean μ and variance σ^2. Consider the random variable $\hat{X}_n$ measuring the sample average:

$$\hat{X}_n = \frac{X_1 + \cdots + X_n}{n}$$

Considering that $\mathbb{E}[a(X+Y)] = a(\mathbb{E}[x] + \mathbb{E}[y])$:

$$\mathbb{E}[\hat{X}_n] = \frac{1}{n}(\mathbb{E}[X_1] + \cdots + \mathbb{E}[X_n]) = p$$

5.4.2 Variance of an average

Consider the random variable $\hat{X}_n$ measuring the sample average. Its variance is computed as $Var[a(X+Y)] = a^2(Var[X] + Var[Y])$ if X and Y are independent:

$$Var[\hat{X}_n] = \frac{1}{n^2}(Var[X_1] + \cdots Var[X_n]) = \frac{\sigma^2}{n}$$

5.4.3 Chebyshev's inequality

Consider a random variable X with mean μ and variance σ^2. For all $a > 0$:

$$Pr[|X - \mu| \geq a] \leq \frac{\sigma^2}{a^2}$$

Considering $a = k\sigma$, for $k > 0$:

$$Pr[|X - \mu| \geq k\sigma] \leq \frac{1}{k^2}$$

Most of the probability mass of a random variable stays within few standard deviations from its mean.

5.4.4 Law of large numbers

Consider a sample $X_1, \ldots, X_n$ instances drawn from a distribution with mean μ and variance σ^2. For any $\varepsilon > 0$ its sample average $\hat{X}_n$ obeys:

$$\lim_{n \to \infty} Pr[|\hat{X}_n - \mu| > \varepsilon] = 0$$

It can be shown using Chebyshev's inequality and the facts that $\mathbb{E}[\hat{X}_n] = \mu$ and $Var[\hat{X}_n] = \frac{\sigma^2}{n}$:

$$Pr[|\hat{X}_n - \mathbb{E}[\bar{X}_n]| \geq \varepsilon] \leq \frac{\sigma^2}{n\varepsilon^2}$$

This tells that the accuracy of an empirical statistic increases with the number of samples.

5.4.5 Central limit theorem

Consider a sample of $X_1, \ldots, X_n$ instances drawn from a distribution with mean μ and variance σ^2. Regardless of the distribution of X, for $n \to \infty$ the distribution of the sample average $\hat{X}_n$ approaches a normal distribution. Its mean approaches μ and its variance $\frac{\sigma^2}{n}$. Thus the normalized sample average"

$$z = \frac{\hat{X}_n - \mu}{\frac{\sigma}{\sqrt{n}}}$$

Approaches a normal distribution $N(0, 1)$.

5.4.5.1 Interpretation

The sum of a sufficiently large sample of random measurements is approximately normally distributed. The form of their distribution can be arbitrary. This justifies the importance of the Normal distribution in real world applications.

5.5 Information theory

5.5.1 Entropy

Consider a discrete set of symbols $\mathcal{V} = \{v_1, \ldots, v_n\}$ with mutually exclusive probabilities. To design a binary code for each symbol minimizing the average length of messages, Shannon and Weaver proved that the optimal code assigns to each symbol a number of bits equal to $-\log P(v_i)$. The entropy of the set of symbols is the expected length of a message encoding a symbol assuming such optimal coding:

$$H[\mathcal{V}] = \mathbb{E}[-\log P(v)] = -\sum_{i=1}^{n} P(v_i) \log P(v_i)$$

5.5.2 Cross entropy

Consider two distributions P and Q over variable X. The cross entropy between P and Q measures the expected number of bits needed to code a symbol sampled from P using Q instead:

$$H(P, Q) = \mathbb{E}_P[-\log Q(v)] = -\sum_{i=1}^{n} P(v_i) \log Q(v_i)$$

It is often used as a loss for binary classification with P true distribution and Q the predicted one.

5.5.3 Relative entropy

Consider two distributions P and Q over variable X. The relative entropy or Kullback-Leibler divergence measures the expected length difference when coding instances sampled from P using Q instead.

$$\begin{aligned} D_{KL}(p||q) &= H(P,Q) - H(P) = \\ &= -\sum_{i=1}^{n} P(v_i) \log Q(v_i) + \sum_{i=1}^{n} P(v_i) \log P(v_i) = \\ &= \sum_{i=1}^{n} P(v_i) \log \frac{P(v_i)}{Q(v_i)} \end{aligned}$$

The KL-divergence is not a distance as it is not symmetric.

5.5.4 Conditional entropy

Consider two variables V and W with possibly different distributions P. The conditional entropy is the entropy remaining for variable W once V is known:

$$\begin{aligned} H(W|V) &= \sum_{v} P(v) H(W|V=v) = \\ &= -\sum_{v} P(v) \sum_{w} P(w|v) \log P(w|v) \end{aligned}$$

5.5.5 Mutual information

Consider two variables V and W with possibly different distributions P. The mutual information or information gain is the reduction in entropy for W once V is known:

$$\begin{aligned} I(W,V) &= H(W) - H(W|V) \\ &= -\sum_{w} p(w) \log p(w) + \sum_{v} P(v) \sum_{w} P(w|v) \log P(w|v) \end{aligned}$$

It is used in selecting the best attribute to use in building a decision tree, where V is the attribute and W is the label.

Chapter 6

Evaluation

6.1 Introduction

Evaluation requires to define the performance measures to be optimized. Performance of learning algorithms cannot be evaluated on the entire domain because of the generalization error, so there is a need for approximation. Performance evaluation is needed for:

- Tuning the hyperparameters of the learning method.
- Evaluating the quality of the learned predictor.
- Computing statistical significance of difference between different learning algorithms.

6.2 Performance measures

6.2.1 Training loss and performance measures

The training loss function measures the cost paid for predicting $f(x)$ for output y. It is designed to boost effectiveness and efficiency of learning algorithm. It is not necessarily the best measure of final performance, for example misclassification cost is never used as it is a piecewise constant no amenable to gradient descent. Multiple performance measures could be used to evaluate different aspects of a learner.

6.2.2 Binary classification

For binary classification the confusion matrix reports the effective label on the rows and the predicted one on the columns. Each entry contains the number of examples having label in row and predicted as column.

- TP true positives: positives predicted as positive.
- FP false positives: negative predicted as positive.
- TN true negative: negative predicted as negative.
- FN false negatives: positives predicted as negatives.

6.2.2.1 Accuracy

Accuracy is the fraction of correctly labelled examples among all predictions. It is one minus the misclassification cost:

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}$$

For strongly unbalanced datasets it is not informative because predictions are dominated by the larger class and predicting everything as negative maximizes accuracy. One way of resolving this problem consists of introducing the rebalancing cost: a single positive counts as $\frac{N}{P}$ where $N = TN + FP$ and $P = TP + FN$.

6.2.2.2 Precision

Precision is the fraction of positives among examples predicted as positives. It measures the precision of the learner when predicting positive:

$$Pre = \frac{TP}{TP + FP}$$

6.2.2.3 Recall or sensitivity

Recall is the fraction of positive examples predicted as positives. It measures the coverage of the learner in returning positive examples:

$$Rec = \frac{TP}{TP + FN}$$

6.2.2.4 F-measure

Precision and recall are complementary: increasing prediction typically reduces recall. F-measures combines the two measures balancing the two aspects with a parameter β that defines the trade-off between precision and recall:

$$F_\beta = \frac{(1 + \beta^2)(Pre + Rec)}{\beta^2 Pre + Rec}$$

If $\beta = 1$ the measure is called F_1 and it is the harmonic mean of precision and recall:

$$F_1 = \frac{2(Pre + Rec)}{Pre + Rec}$$

6.2.2.5 Precision-recall curve

Classifiers often provide a confidence in the prediction and a hard decision is made setting a threshold on the classifier. Accuracy, precision, recall and F_1 all measures performance of a classifier for a specific threshold. It is possible to change the threshold if the interest is in maximizing a specific performance. By varying the threshold from minimum to maximum possible values we obtain a curve of performance measures. This curve can be shown plotting one measure like recall against the complementary one like precision. It is possible to investigate performance of the learner in different scenarios. The area under this curve can be used as a single aggregate value that combines performance of the algorithm for all possible threshold.

6.2.3 Multiclass classification

For multiclass classification the confusion matrix is a generalized evasion of the binary one such that n_{ij} is the number of examples with class y_i predicted as y_j. The main diagonal contains true positives for each class. The sum of off-diagonal elements along a column is the number of false positive for the column label and the sum of off-diagonal elements along a row is the number of false negatives for the raw label:

- $FP_i = \sum_{j \neq i} n_{ji}$
- $FN_i = \sum_{j \neq i} n_{ij}$

6.2.3.1 Muliclass accuracy

Accuracy, precision, recall and F_1 carry over to a per-class measure considering as negative examples from other classes:

- $Pre_i = \frac{n_{ii}}{n_{ii}+FP_i}$
- $Rec_i = \frac{n_{ii}}{n_{ii}+FN_i}$

Multiclass accuracy is the overall fraction of correctly classified examples:

$$MAcc = \frac{\sum_i n_{ii}}{\sum_i \sum_j n_i}$$

6.2.4 Regression

6.2.4.1 Root mean squared error

The root mean squared error for dataset $\mathcal{D}$ with $n = |\mathcal{D}|$ is:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(f(x_i) - y_i)^2}$$

6.2.4.2 Pearson correlation coefficient

The Pearson correlation coefficient for random variable X and Y is:

$$\rho = \frac{cov(X,Y)}{\sigma_X \sigma_Y} = \frac{\mathbb{E}[(X - \bar{X})(Y - \bar{Y}]}{\sqrt{\mathbb{E}[(X - \bar{X})^2]\mathbb{E}[(Y - \bar{Y})^2]}}$$

For regression on $\mathcal{D}$ it becomes:

$$\rho = frac\sum_{i=1}^{n}(f(x_i) - \bar{f}(x_i))(y_i - \bar{y}_i)\sqrt{\sum_{i=1}^{n}(f(x_i) - \bar{f}(x_i))^2 \sum_{i=1}^{n}(y_i - \bar{y}_i)^2}$$

Where $\bar{z}$ is the average of z on $\mathcal{D}$.

6.2.4.3 Hold-out procedure

Computing the performance measure on training set would be optimistically biased, so there is a need to retain an independent set on which to compute performance:

- Validation set: when used to estimate performance of different algorithmic settings.
- Test set: when used to estimate final performance of selected model.

Hold-out procedure depends on the specific test and validation set chosen.

6.2.4.4 K-fold cross validation

In the k-fold cross validation $\mathcal{D}$ is split in k equal sized disjoint subsets $\mathcal{D}_i$. Then for $i \in [1, k]$L

1. Train predictor on $\mathcal{T} = \mathcal{D} \backslash \mathcal{D}_i$.
2. Compute score S of predictor $L(\mathcal{T}_i)$ on test set $\mathcal{D}_i$: $S_i = S_{\mathcal{D}_i}[L(\mathcal{T}_i)]$.

Then the average score across folds is returned:

$$S = \frac{1}{k} \sum_{i=1}^{k} S_i$$