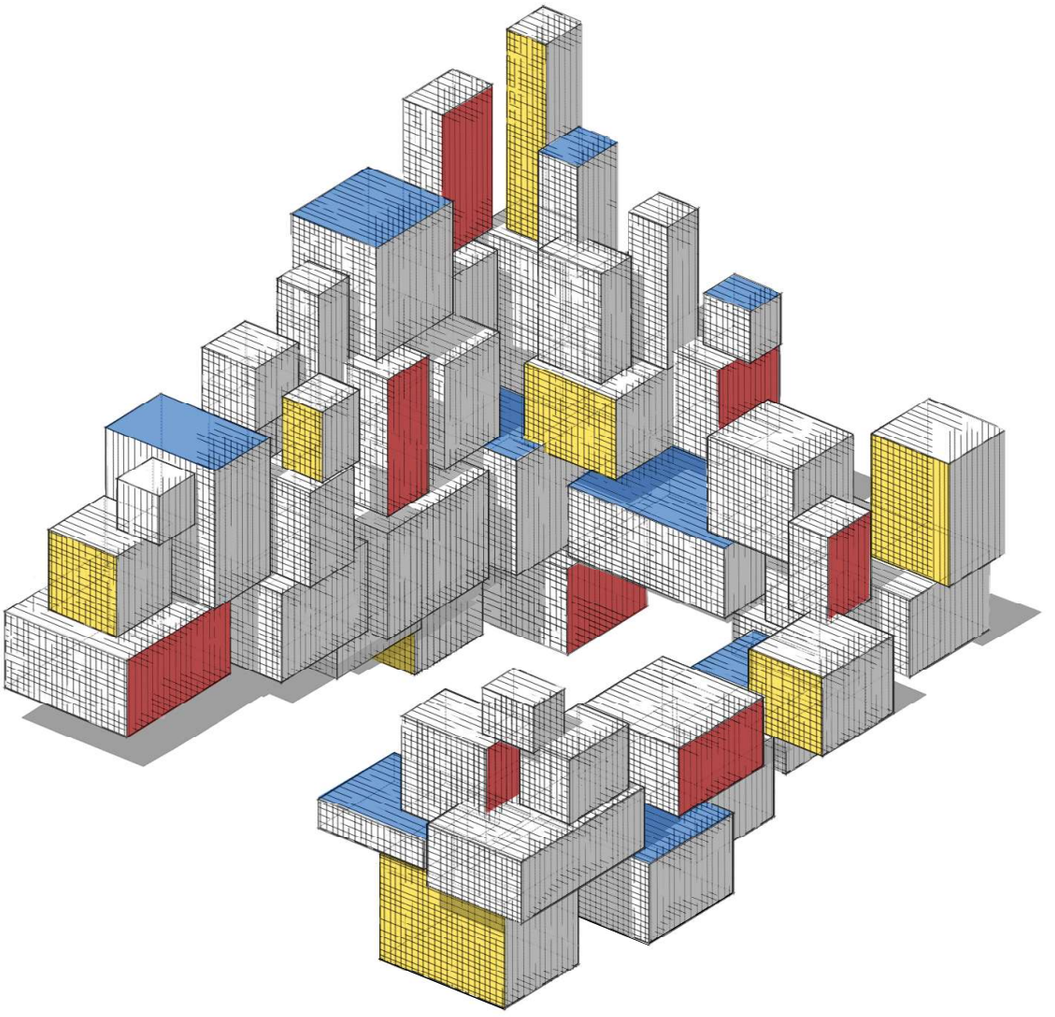
Data Science and Machine Learning

Mathematical and Statistical Methods



Dirk P. Kroese, Zdravko I. Botev, Thomas Taimre, Radislav Vaisman

8th May 2022

To my wife and daughters: Lesley, Elise, and Jessica

— DPK

To Sarah, Sofia, and my parents

— ZIB

To my grandparents: Arno, Harry, Juta, and Maila

— TT

To Valerie

— RV

CONTENTS

PREFACE

In our present world of automation, cloud computing, algorithms, artificial intelligence, and big data, few topics are as relevant as *data science* and *machine learning*. Their recent popularity lies not only in their applicability to real-life questions, but also in their natural blending of many different disciplines, including mathematics, statistics, computer science, engineering, science, and finance.

To someone starting to learn these topics, the multitude of computational techniques and mathematical ideas may seem overwhelming. Some may be satisfied with only learning how to use off-the-shelf recipes to apply to practical situations. But what if the assumptions of the black-box recipe are violated? Can we still trust the results? How should the algorithm be adapted? To be able to truly understand data science and machine learning it is important to appreciate the underlying mathematics and statistics, as well as the resulting algorithms.

The purpose of this book is to provide an accessible, yet comprehensive, account of data science and machine learning. It is intended for anyone interested in gaining a better understanding of the mathematics and statistics that underpin the rich variety of ideas and machine learning algorithms in data science. Our viewpoint is that computer languages come and go, but the underlying key ideas and algorithms will remain forever and will form the basis for future developments.

Before we turn to a description of the topics in this book, we would like to say a few words about its philosophy. This book resulted from various courses in data science and machine learning at the Universities of Queensland and New South Wales, Australia. When we taught these courses, we noticed that students were eager to learn not only how to apply algorithms but also to understand how these algorithms actually work. However, many existing textbooks assumed either too much background knowledge (e.g., measure theory and functional analysis) or too little (everything is a black box), and the information overload from often disjointed and contradictory internet sources made it more difficult for students to gradually build up their knowledge and understanding. We therefore wanted to write a book about data science and machine learning that can be read as a linear story, with a substantial "backstory" in the appendices. The main narrative starts very simply and builds up gradually to quite an advanced level. The backstory contains all the necessary

background, as well as additional information, from linear algebra and functional analysis (Appendix A), multivariate differentiation and optimization (Appendix B), and probability and statistics (Appendix C). Moreover, to make the abstract ideas come alive, we believe it is important that the reader sees actual implementations of the algorithms, directly translated from the theory. After some deliberation we have chosen Python as our programming language. It is freely available and has been adopted as the programming language of choice for many practitioners in data science and machine learning. It has many useful packages for data manipulation (often ported from R) and has been designed to be easy to program. A gentle introduction to Python is given in Appendix D.

To keep the book manageable in size we had to be selective in our choice of topics. Important ideas and connections between various concepts are highlighted via *keywords* and page references (indicated by a ☞) in the margin. Key definitions and theorems are highlighted in boxes. Whenever feasible we provide proofs of theorems. Finally, we place great importance on *notation*. It is often the case that once a consistent and concise system of notation is in place, seemingly difficult ideas suddenly become obvious. We use different fonts to distinguish between different types of objects. Vectors are denoted by letters in boldface italics, $\boldsymbol{x}$, $\boldsymbol{X}$, and matrices by uppercase letters in boldface roman font, $\mathbf{A}$, $\mathbf{K}$. We also distinguish between random vectors and their values by using upper and lower case letters, e.g., $\boldsymbol{X}$ (random vector) and $\boldsymbol{x}$ (its value or outcome). Sets are usually denoted by calligraphic letters $\mathcal{G}, \mathcal{H}$. The symbols for probability and expectation are $\mathbb{P}$ and $\mathbb{E}$, respectively. Distributions are indicated by sans serif font, as in Bin and Gamma; exceptions are the ubiquitous notations $\mathcal{N}$ and $\mathcal{U}$ for the normal and uniform distributions. A summary of the most important symbols and abbreviations is given on Pages xvii–xxi.

KEYWORDS

☞ xvii

Data science provides the language and techniques necessary for understanding and dealing with data. It involves the design, collection, analysis, and interpretation of numerical data, with the aim of extracting patterns and other useful information. Machine learning, which is closely related to data science, deals with the design of algorithms and computer resources to learn from data. The organization of the book follows roughly the typical steps in a data science project: Gathering data to gain information about a research question; cleaning, summarization, and visualization of the data; modeling and analysis of the data; translating decisions about the model into decisions and predictions about the research question. As this is a mathematics and statistics oriented book, most emphasis will be on modeling and analysis.

We start in Chapter 1 with the reading, structuring, summarization, and visualization of data using the data manipulation package `pandas` in Python. Although the material covered in this chapter requires no mathematical knowledge, it forms an obvious starting point for data science: to better understand the nature of the available data. In Chapter 2, we introduce the main ingredients of *statistical learning*. We distinguish between *supervised* and *unsupervised* learning techniques, and discuss how we can assess the predictive performance of (un)supervised learning methods. An important part of statistical learning is the *modeling* of data. We introduce various useful models in data science including linear, multivariate Gaussian, and Bayesian models. Many algorithms in machine learning and data science make use of Monte Carlo techniques, which is the topic of Chapter 3. Monte Carlo can be used for simulation, estimation, and optimization. Chapter 4 is concerned with unsupervised learning, where we discuss techniques such as density estimation, clustering, and principal component analysis. We then turn our attention to supervised learning

in Chapter 5, and explain the ideas behind a broad class of regression models. Therein, we also describe how Python's `statsmodels` package can be used to define and analyze linear models. Chapter 6 builds upon the previous regression chapter by developing the powerful concepts of kernel methods and regularization, which allow the fundamental ideas of Chapter 5 to be expanded in an elegant way, using the theory of reproducing kernel Hilbert spaces. In Chapter 7, we proceed with the classification task, which also belongs to the supervised learning framework, and consider various methods for classification, including Bayes classification, linear and quadratic discriminant analysis, K-nearest neighbors, and support vector machines. In Chapter 8 we consider versatile methods for regression and classification that make use of tree structures. Finally, in Chapter 9, we consider the workings of neural networks and deep learning, and show that these learning algorithms have a simple mathematical interpretation. An extensive range of exercises is provided at the end of each chapter.

Python code and data sets for each chapter can be downloaded from the GitHub site:
https://github.com/DSML-book

Acknowledgments

Some of the Python code for Chapters 1 and 5 was adapted from [73]. We thank Benoit Liquet for making this available, and Lauren Jones for translating the R code into Python.

We thank all who through their comments, feedback, and suggestions have contributed to this book, including Qibin Duan, Luke Taylor, Rémi Mouzayek, Harry Goodman, Bryce Stansfield, Ryan Tongs, Dillon Steyl, Bill Rudd, Nan Ye, Christian Hirsch, Chris van der Heide, Sarat Moka, Aapeli Vuorinen, Joshua Ross, Giang Nguyen, and the anonymous referees. David Grubbs deserves a special accollade for his professionalism and attention to detail in his role as Editor for this book.

The book was test-run during the 2019 *Summer School of the Australian Mathematical Sciences Institute*. More than 80 bright upper-undergraduate (Honours) students used the book for the course *Mathematical Methods for Machine Learning*, taught by Zdravko Botev. We are grateful for the valuable feedback that they provided.

Our special thanks go out to Robert Salomone, Liam Berry, Robin Carrick, and Sam Daley, who commented in great detail on earlier versions of the entire book and wrote and improved our Python code. Their enthusiasm, perceptiveness, and kind assistance have been invaluable.

Of course, none of this work would have been possible without the loving support, patience, and encouragement from our families, and we thank them with all our hearts.

This book was financially supported by the Australian Research Council *Centre of Excellence for Mathematical & Statistical Frontiers*, under grant number CE140100049.

Dirk Kroese, Zdravko Botev,
Thomas Taimre, and Radislav Vaisman
Brisbane and Sydney

NOTATION

We could, of course, use any notation we want; do not laugh at notations; invent them, they are powerful. In fact, mathematics is, to a large extent, invention of better notations.

Richard P. Feynman

We have tried to use a notation system that is, in order of importance, simple, descriptive, consistent, and compatible with historical choices. Achieving all of these goals all of the time would be impossible, but we hope that our notation helps to quickly recognize the type or "flavor" of certain mathematical objects (vectors, matrices, random vectors, probability measures, etc.) and clarify intricate ideas.

We make use of various typographical aids, and it will be beneficial for the reader to be aware of some of these.

• Boldface font is used to indicate composite objects, such as column vectors $\boldsymbol{x} = [x_1, \ldots, x_n]^\top$ and matrices $\mathbf{X} = [x_{ij}]$. Note also the difference between the upright bold font for matrices and the slanted bold font for vectors.

• Random variables are generally specified with upper case roman letters X, Y, Z and their outcomes with lower case letters x, y, z. Random vectors are thus denoted in upper case slanted bold font: $\boldsymbol{X} = [X_1, \ldots, X_n]^\top$.

• Sets of vectors are generally written in calligraphic font, such as $\mathcal{X}$, but the set of real numbers uses the common blackboard bold font $\mathbb{R}$. Expectation and probability also use the latter font.

• Probability distributions use a sans serif font, such as Bin and Gamma. Exceptions to this rule are the "standard" notations $\mathcal{N}$ and $\mathcal{U}$ for the normal and uniform distributions.

• We often omit brackets when it is clear what the argument is of a function or operator. For example, we prefer $\mathbb{E}X^2$ to $\mathbb{E}[X^2]$.

• We employ color to emphasize that certain words refer to a `dataset`, `function`, or `package` in Python. All code is written in `typewriter` font. To be compatible with past notation choices, we introduced a special blue symbol $\mathbf{X}$ for the model (design) matrix of a linear model.

• Important notation such as $\mathcal{T}$, g, g^* is often defined in a mnemonic way, such as $\mathcal{T}$ for "training", g for "guess", g^* for the "star" (that is, optimal) guess, and ℓ for "loss".

• We will occasionally use a Bayesian notation convention in which the *same* symbol is used to denote different (conditional) probability densities. In particular, instead of writing $f_X(x)$ and $f_{X|Y}(x|y)$ for the probability density function (pdf) of X and the conditional pdf of X given Y, we simply write $f(x)$ and $f(x|y)$. This particular style of notation can be of great descriptive value, despite its apparent ambiguity.

General font/notation rules

x	scalar
$\boldsymbol{x}$	vector
$\boldsymbol{X}$	random vector
$\mathbf{X}$	matrix
$\mathcal{X}$	set
$\widehat{x}$	estimate or approximation
x^*	optimal
$\overline{x}$	average

Common mathematical symbols

$\forall$	for all
$\exists$	there exists
$\propto$	is proportional to
$\perp$	is perpendicular to
$\sim$	is distributed as
$\overset{\text{iid}}{\sim}$, $\sim_{\text{iid}}$	are independent and identically distributed as
$\overset{\text{approx.}}{\sim}$	is approximately distributed as
∇f	gradient of f
$\nabla^2 f$	Hessian of f
$f \in C^p$	f has continuous derivatives of order p
$\approx$	is approximately
$\simeq$	is asymptotically
$\ll$	is much smaller than
$\oplus$	direct sum

$\odot$	elementwise product
$\cap$	intersection
$\cup$	union
$:=$, $=:$	is defined as
$\xrightarrow{\text{a.s.}}$	converges almost surely to
$\xrightarrow{\text{d}}$	converges in distribution to
$\xrightarrow{\mathbb{P}}$	converges in probability to
$\xrightarrow{L_p}$	converges in L_p-norm to
$\|\cdot\|$	Euclidean norm
$\lceil x \rceil$	smallest integer larger than x
$\lfloor x \rfloor$	largest integer smaller than x
x_+	$\max\{x, 0\}$

Matrix/vector notation

$\mathbf{A}^\top$, $\boldsymbol{x}^\top$	transpose of matrix $\mathbf{A}$ or vector $\boldsymbol{x}$
$\mathbf{A}^{-1}$	inverse of matrix $\mathbf{A}$
$\mathbf{A}^+$	pseudo-inverse of matrix $\mathbf{A}$
$\mathbf{A}^{-\top}$	inverse of matrix $\mathbf{A}^\top$ or transpose of $\mathbf{A}^{-1}$
$\mathbf{A} \succ 0$	matrix $\mathbf{A}$ is positive definite
$\mathbf{A} \succeq 0$	matrix $\mathbf{A}$ is positive semidefinite
$\dim(\boldsymbol{x})$	dimension of vector $\boldsymbol{x}$
$\det(\mathbf{A})$	determinant of matrix $\mathbf{A}$
$\lvert\mathbf{A}\rvert$	absolute value of the determinant of matrix $\mathbf{A}$
$\operatorname{tr}(\mathbf{A})$	trace of matrix $\mathbf{A}$

Reserved letters and words

$\mathbb{C}$	set of complex numbers
d	differential symbol
$\mathbb{E}$	expectation
e	the number 2.71828 . . .
f	probability density (discrete or continuous)
g	prediction function
$\mathbb{1}\{A\}$ or $\mathbb{1}_A$	indicator function of set A
i	the square root of -1
ℓ	risk: expected loss

Loss	loss function
ln	(natural) logarithm
$\mathbb{N}$	set of natural numbers $\{0, 1, \ldots\}$
$\mathcal{O}$	big-O order symbol: $f(x) = \mathcal{O}(g(x))$ if $\lvert f(x)\rvert \leqslant \alpha g(x)$ for some constant α as $x \to a$
o	little-o order symbol: $f(x) = o(g(x))$ if $f(x)/g(x) \to 0$ as $x \to a$
$\mathbb{P}$	probability measure
π	the number $3.14159\ldots$
$\mathbb{R}$	set of real numbers (one-dimensional Euclidean space)
$\mathbb{R}^n$	n-dimensional Euclidean space
$\mathbb{R}_+$	positive real line: $[0, \infty)$
τ	deterministic training set
$\mathcal{T}$	random training set
$\mathbf{X}$	model (design) matrix
$\mathbb{Z}$	set of integers $\{\ldots, -1, 0, 1, \ldots\}$

Probability distributions

Ber	Bernoulli
Beta	beta
Bin	binomial
Exp	exponential
Geom	geometric
Gamma	gamma
F	Fisher–Snedecor F
$\mathcal{N}$	normal or Gaussian
Pareto	Pareto
Poi	Poisson
t	Student's t
$\mathcal{U}$	uniform

Abbreviations and acronyms

cdf	cumulative distribution function
CMC	crude Monte Carlo
CE	cross-entropy
EM	expectation–maximization
GP	Gaussian process
KDE	Kernel density estimate/estimator

KL	Kullback–Leibler
KKT	Karush–Kuhn–Tucker
iid	independent and identically distributed
MAP	maximum *a posteriori*
MCMC	Markov chain Monte Carlo
MLE	maximum likelihood estimator/estimate
OOB	out-of-bag
PCA	principal component analysis
pdf	probability density function (discrete or continuous)
SVD	singular value decomposition

CHAPTER 1

IMPORTING, SUMMARIZING, AND VISUALIZING DATA

This chapter describes where to find useful data sets, how to load them into Python, and how to (re)structure the data. We also discuss various ways in which the data can be summarized via tables and figures. Which type of plots and numerical summaries are appropriate depends on the type of the variable(s) in play. Readers unfamiliar with Python are advised to read Appendix D first.

1.1 Introduction

Data comes in many shapes and forms, but can generally be thought of as being the result of some random experiment — an experiment whose outcome cannot be determined in advance, but whose workings are still subject to analysis. Data from a random experiment are often stored in a table or spreadsheet. A statistical convention is to denote variables — often called *features* — as *columns* and the individual items (or units) as *rows*. It is useful to think of three types of columns in such a spreadsheet:

FEATURES

1. The first column is usually an identifier or index column, where each unit/row is given a unique name or ID.

2. Certain columns (features) can correspond to the design of the experiment, specifying, for example, to which experimental group the unit belongs. Often the entries in these columns are *deterministic*; that is, they stay the same if the experiment were to be repeated.

3. Other columns represent the observed measurements of the experiment. Usually, these measurements exhibit *variability*; that is, they would change if the experiment were to be repeated.

There are many data sets available from the Internet and in software packages. A well-known repository of data sets is the Machine Learning Repository maintained by the University of California at Irvine (UCI), found at https://archive.ics.uci.edu/.

These data sets are typically stored in a CSV (comma separated values) format, which can be easily read into Python. For example, to access the **abalone** data set from this website with Python, download the file to your working directory, import the **pandas** package via

```
import pandas as pd
```

and read in the data as follows:

```
abalone = pd.read_csv('abalone.data',header = None)
```

It is important to add `header = None`, as this lets Python know that the first line of the CSV does not contain the names of the features, as it assumes so by default. The data set was originally used to predict the age of abalone from physical measurements, such as shell weight and diameter.

Another useful repository of over 1000 data sets from various packages in the R programming language, collected by Vincent Arel-Bundock, can be found at:

https://vincentarelbundock.github.io/Rdatasets/datasets.html.

For example, to read Fisher's famous **iris** data set from R's `datasets` package into Python, type:

```
urlprefix = 'https://vincentarelbundock.github.io/Rdatasets/csv/'
dataname = 'datasets/iris.csv'
iris = pd.read_csv(urlprefix + dataname)
```

The **iris** data set contains four physical measurements (sepal/petal length/width) on 50 specimens (each) of 3 species of iris: setosa, versicolor, and virginica. Note that in this case the headers are included. The output of **read_csv** is a `DataFrame` object, which is **pandas**'s implementation of a spreadsheet; see Section D.12.1. The `DataFrame` method **head** gives the first few rows of the `DataFrame`, including the feature names. The number of rows can be passed as an argument and is 5 by default. For the **iris** `DataFrame`, we have:

☞ 487

```
iris.head()
```

```
   Unnamed: 0  Sepal.Length   ...    Petal.Width  Species
0           1           5.1   ...            0.2   setosa
1           2           4.9   ...            0.2   setosa
2           3           4.7   ...            0.2   setosa
3           4           4.6   ...            0.2   setosa
4           5           5.0   ...            0.2   setosa

[5 rows x 6 columns]
```

The names of the features can be obtained via the `columns` attribute of the `DataFrame` object, as in `iris.columns`. Note that the first column is a duplicate index column, whose name (assigned by **pandas**) is `'Unnamed: 0'`. We can drop this column and reassign the `iris` object as follows:

```
iris = iris.drop('Unnamed: 0',1)
```

The data for each feature (corresponding to its specific name) can be accessed by using Python's *slicing* notation `[]`. For example, the object `iris['Sepal.Length']` contains the 150 sepal lengths.

The first three rows of the **abalone** data set from the UCI repository can be found as follows:

```
abalone.head(3)
```

	0	1	2	3	4	5	6	7	8
0	M	0.455	0.365	0.095	0.5140	0.2245	0.1010	0.150	15
1	M	0.350	0.265	0.090	0.2255	0.0995	0.0485	0.070	7
2	F	0.530	0.420	0.135	0.6770	0.2565	0.1415	0.210	9

Here, the missing headers have been assigned according to the order of the natural numbers. The names should correspond to Sex, Length, Diameter, Height, Whole weight, Shucked weight, Viscera weight, Shell weight, and Rings, as described in the file with the name `abalone.names` on the UCI website. We can manually add the names of the features to the `DataFrame` by reassigning the columns attribute, as in:

```
abalone.columns = ['Sex', 'Length', 'Diameter', 'Height',
'Whole weight','Shucked weight', 'Viscera weight', 'Shell weight',
'Rings']
```

1.2 Structuring Features According to Type

We can generally classify features as either quantitative or qualitative. *Quantitative* features possess "numerical quantity", such as height, age, number of births, etc., and can either be *continuous* or *discrete*. Continuous quantitative features take values in a continuous range of possible values, such as height, voltage, or crop yield; such features capture the idea that measurements can always be made more precisely. Discrete quantitative features have a countable number of possibilities, such as a count.

QUANTITATIVE

In contrast, *qualitative* features do not have a numerical meaning, but their possible values can be divided into a fixed number of categories, such as {M,F} for gender or {blue, black, brown, green} for eye color. For this reason such features are also called *categorical*. A simple rule of thumb is: if it does not make sense to average the data, it is categorical. For example, it does not make sense to average eye colors. Of course it is still possible to represent categorical data with numbers, such as 1 = blue, 2 = black, 3 = brown, but such numbers carry no quantitative meaning. Categorical features are often called *factors*.

QUALITATIVE

CATEGORICAL

FACTORS

When manipulating, summarizing, and displaying data, it is important to correctly specify the type of the variables (features). We illustrate this using the `nutrition_elderly` data set from [73], which contains the results of a study involving nutritional measurements of thirteen features (columns) for 226 elderly individuals (rows). The data set can be obtained from:

http://www.biostatisticien.eu/springeR/nutrition_elderly.xls.

Excel files can be read directly into **pandas** via the **read_excel** method:

```
xls = 'http://www.biostatisticien.eu/springeR/nutrition_elderly.xls'
nutri = pd.read_excel(xls)
```

This creates a `DataFrame` object **nutri**. The first three rows are as follows:

```
pd.set_option('display.max_columns', 8) # to fit display
nutri.head(3)
```

```
   gender  situation  tea ...   cooked_fruit_veg  chocol  fat
0       2          1    0 ...                  4       5    6
1       2          1    1 ...                  5       1    4
2       2          1    0 ...                  2       5    4

[3 rows x 13 columns]
```

You can check the type (or structure) of the variables via the **info** method of **nutri**.

```
nutri.info()
```

```
 <class 'pandas.core.frame.DataFrame'>
RangeIndex: 226 entries, 0 to 225
Data columns (total 13 columns):
gender              226 non-null int64
situation           226 non-null int64
tea                 226 non-null int64
coffee              226 non-null int64
height              226 non-null int64
weight              226 non-null int64
age                 226 non-null int64
meat                226 non-null int64
fish                226 non-null int64
raw_fruit           226 non-null int64
cooked_fruit_veg    226 non-null int64
chocol              226 non-null int64
fat                 226 non-null int64
dtypes: int64(13)
memory usage: 23.0 KB
```

All 13 features in **nutri** are (at the moment) interpreted by Python as *quantitative* variables, indeed as integers, simply because they have been entered as whole numbers. The *meaning* of these numbers becomes clear when we consider the description of the features, given in Table 1.2. Table 1.1 shows how the variable types should be classified.

Table 1.1: The feature types for the data frame **nutri**.

Qualitative	`gender`, `situation`, `fat`
	`meat`, `fish`, `raw_fruit`, `cooked_fruit_veg`, `chocol`
Discrete quantitative	`tea`, `coffee`
Continuous quantitative	`height`, `weight`, `age`

Note that the categories of the qualitative features in the second row of Table 1.1, `meat`, . . . , `chocol` have a natural order. Such qualitative features are sometimes called *ordinal*, in

Table 1.2: Description of the variables in the nutritional study [73].

Feature	**Description**	**Unit** or **Coding**
`gender`	Gender	1=Male; 2=Female
`situation`	Family status	1=Single 2=Living with spouse 3=Living with family 4=Living with someone else
`tea`	Daily consumption of tea	Number of cups
`coffee`	Daily consumption of coffee	Number of cups
`height`	Height	cm
`weight`	Weight (actually: mass)	kg
`age`	Age at date of interview	Years
`meat`	Consumption of meat	0=Never 1=Less than once a week 2=Once a week 3=2–3 times a week 4=4–6 times a week 5=Every day
`fish`	Consumption of fish	As in `meat`
`raw_fruit`	Consumption of raw fruits	As in `meat`
`cooked_fruit_veg`	Consumption of cooked fruits and vegetables	As in `meat`
`chocol`	Consumption of chocolate	As in `meat`
`fat`	Type of fat used for cooking	1=Butter 2=Margarine 3=Peanut oil 4=Sunflower oil 5=Olive oil 6=Mix of vegetable oils (e.g., Isio4) 7=Colza oil 8=Duck or goose fat

contrast to qualitative features without order, which are called *nominal*. We will not make such a distinction in this book.

We can modify the Python value and type for each categorical feature, using the `replace` and `astype` methods. For categorical features, such as `gender`, we can replace the value 1 with `'Male'` and 2 with `'Female'`, and change the type to `'category'` as follows.

```
DICT = {1:'Male', 2:'Female'} # dictionary specifies replacement
nutri['gender'] = nutri['gender'].replace(DICT).astype('category')
```

The structure of the other categorical-type features can be changed in a similar way. Continuous features such as `height` should have type `float`:

```
nutri['height'] = nutri['height'].astype(float)
```

We can repeat this for the other variables (see Exercise 2) and save this modified data frame as a CSV file, by using the **pandas** method **to_csv**.

```
nutri.to_csv('nutri.csv',index=False)
```

1.3 Summary Tables

It is often useful to summarize a large spreadsheet of data in a more condensed form. A table of counts or a table of frequencies makes it easier to gain insight into the underlying distribution of a variable, especially if the data are qualitative. Such tables can be obtained with the methods **describe** and **value_counts**.

As a first example, we load the **nutri** DataFrame, which we restructured and saved (see previous section) as `'nutri.csv'`, and then construct a summary for the feature (column) `'fat'`.

```
nutri = pd.read_csv('nutri.csv')
nutri['fat'].describe()
```

```
count            226
unique             8
top        sunflower
freq              68
Name: fat, dtype: object
```

We see that there are 8 different types of fat used and that sunflower has the highest count, with 68 out of 226 individuals using this type of cooking fat. The method **value_counts** gives the counts for the different fat types.

```
nutri['fat'].value_counts()
```

```
sunflower    68
peanut       48
olive        40
margarine    27
Isio4        23
butter       15
duck          4
colza         1
Name: fat, dtype: int64
```

Column labels are also attributes of a DataFrame, and `nutri.fat`, for example, is exactly the same object as `nutri['fat']`.

It is also possible to use **crosstab** to *cross tabulate* between two or more variables, giving a *contingency table*:

CROSS TABULATE

```
pd.crosstab(nutri.gender, nutri.situation)
```

```
situation  Couple  Family  Single
gender
Female         56       7      78
Male           63       2      20
```

We see, for example, that the proportion of single men is substantially smaller than the proportion of single women in the data set of elderly people. To add row and column totals to a table, use `margins=True`.

```
pd.crosstab(nutri.gender, nutri.situation, margins=True)
```

```
situation  Couple  Family  Single  All
gender
Female         56       7      78  141
Male           63       2      20   85
All           119       9      98  226
```

1.4 Summary Statistics

In the following, $\boldsymbol{x} = [x_1, \ldots, x_n]^\top$ is a column vector of n numbers. For our **nutri** data, the vector $\boldsymbol{x}$ could, for example, correspond to the heights of the $n = 226$ individuals.

The *sample mean* of $\boldsymbol{x}$, denoted by $\overline{x}$, is simply the average of the data values:

SAMPLE MEAN

$$\overline{x} = \frac{1}{n} \sum_{i=1}^{n} x_i.$$

Using the **mean** method in Python for the **nutri** data, we have, for instance:

```
nutri['height'].mean()
```

```
163.96017699115043
```

The *p-sample quantile* ($0 < p < 1$) of $\boldsymbol{x}$ is a value x such that at least a fraction p of the data is less than or equal to x and at least a fraction $1 - p$ of the data is greater than or equal to x. The *sample median* is the sample 0.5-quantile. The p-sample quantile is also called the $100 \times p$ *percentile*. The 25, 50, and 75 sample percentiles are called the first, second, and third *quartiles* of the data. For the **nutri** data they are obtained as follows.

SAMPLE QUANTILE

SAMPLE MEDIAN

QUARTILES

```
nutri['height'].quantile(q=[0.25,0.5,0.75])
```

```
0.25    157.0
0.50    163.0
0.75    170.0
```

SAMPLE RANGE

SAMPLE VARIANCE

The sample mean and median give information about the *location* of the data, while the distance between sample quantiles (say the 0.1 and 0.9 quantiles) gives some indication of the *dispersion* (spread) of the data. Other measures for dispersion are the *sample range*, $\max_i x_i - \min_i x_i$, the *sample variance*

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2, \tag{1.1}$$

SAMPLE STANDARD DEVIATION

☞ 457

and the *sample standard deviation* $s = \sqrt{s^2}$. For the **nutri** data, the range (in cm) is:

```
nutri['height'].max() - nutri['height'].min()
```

```
48.0
```

The variance (in cm^2) is:

```
round(nutri['height'].var(), 2)  # round to two decimal places
```

```
81.06
```

And the standard deviation can be found via:

```
round(nutri['height'].std(), 2)
```

```
9.0
```

We already encountered the **describe** method in the previous section for summarizing qualitative features, via the most frequent count and the number of unique elements. When applied to a *quantitative* feature, it returns instead the minimum, maximum, mean, and the three quartiles. For example, the `'height'` feature in the **nutri** data has the following summary statistics.

```
nutri['height'].describe()
```

```
count    226.000000
mean     163.960177
std        9.003368
min      140.000000
25\%      157.000000
50\%      163.000000
75\%      170.000000
max      188.000000
Name: height, dtype: float64
```

1.5 Visualizing Data

In this section we describe various methods for visualizing data. The main point we would like to make is that the way in which variables are visualized should always be adapted to the variable types; for example, qualitative data should be plotted differently from quantitative data.

For the rest of this section, it is assumed that **matplotlib.pyplot**, **pandas**, and **numpy**, have been imported in the Python code as follows.

```
import matplotlib.pyplot as plt
import pandas as pd
import numpy as np
```

1.5.1 Plotting Qualitative Variables

Suppose we wish to display graphically how many elderly people are living by themselves, as a couple, with family, or other. Recall that the data are given in the `situation` column of our **nutri** data. Assuming that we already *restructured the data*, as in Section 1.2, we can make a *barplot* of the number of people in each category via the **plt.bar** function of the standard **matplotlib** plotting library. The inputs are the x-axis positions, heights, and widths of each bar respectively.

☞ 3

BARPLOT

```
width = 0.35 # the width of the bars
x = [0, 0.8, 1.6] # the bar positions on x-axis
situation_counts=nutri['situation'].value_counts()
plt.bar(x, situation_counts, width, edgecolor = 'black')
plt.xticks(x, situation_counts.index)
plt.show()
```

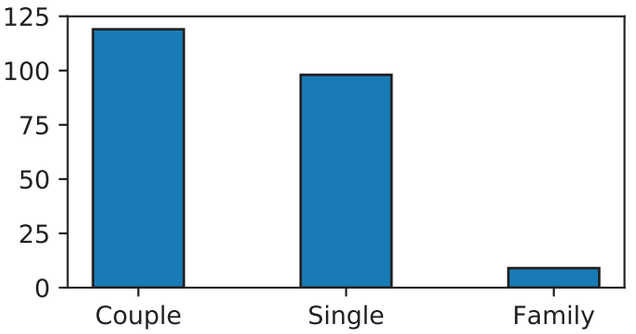


Figure 1.1: Barplot for the qualitative variable `'situation'`.

1.5.2 Plotting Quantitative Variables

We now present a few useful methods for visualizing quantitative data, again using the **nutri** data set. We will first focus on continuous features (e.g., `'age'`) and then add some specific graphs related to discrete features (e.g., `'tea'`). The aim is to describe the variability present in a single feature. This typically involves a central tendency, where observations tend to gather around, with fewer observations further away. The main aspects of the distribution are the *location* (or center) of the variability, the *spread* of the variability (how far the values extend from the center), and the *shape* of the variability; e.g., whether or not values are spread symmetrically on either side of the center.

1.5.2.1 Boxplot

BOXPLOT

A *boxplot* can be viewed as a graphical representation of the five-number summary of the data consisting of the minimum, maximum, and the first, second, and third quartiles. Figure 1.2 gives a boxplot for the `'age'` feature of the **nutri** data.

```
plt.boxplot(nutri['age'],widths=width,vert=False)
plt.xlabel('age')
plt.show()
```

The `widths` parameter determines the width of the boxplot, which is by default plotted vertically. Setting `vert=False` plots the boxplot horizontally, as in Figure 1.2.

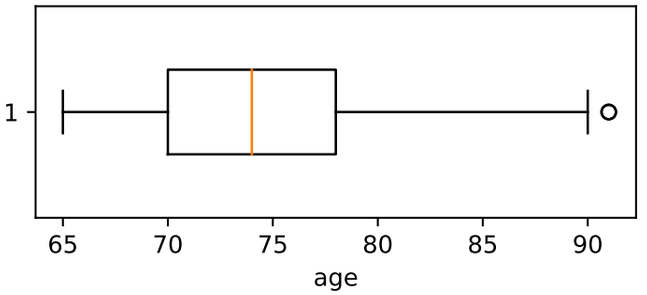


Figure 1.2: Boxplot for `'age'`.

The box is drawn from the first quartile (Q_1) to the third quartile (Q_3). The vertical line inside the box signifies the location of the median. So-called "whiskers" extend to either side of the box. The size of the box is called the *interquartile range*: IQR = $Q_3 - Q_1$. The left whisker extends to the largest of (a) the minimum of the data and (b) $Q_1 - 1.5\,\text{IQR}$. Similarly, the right whisker extends to the smallest of (a) the maximum of the data and (b) $Q_3 + 1.5\,\text{IQR}$. Any data point outside the whiskers is indicated by a small hollow dot, indicating a suspicious or deviant point (outlier). Note that a boxplot may also be used for discrete quantitative features.

1.5.2.2 Histogram

HISTOGRAM

A *histogram* is a common graphical representation of the distribution of a quantitative feature. We start by breaking the range of the values into a number of *bins* or *classes*. We tally the counts of the values falling in each bin and then make the plot by drawing rectangles whose bases are the bin intervals and whose heights are the counts. In Python we can use the function **plt.hist**. For example, Figure 1.3 shows a histogram of the 226 ages in **nutri**, constructed via the following Python code.

```
weights = np.ones_like(nutri.age)/nutri.age.count()
plt.hist(nutri.age,bins=9,weights=weights,facecolor='cyan',
         edgecolor='black', linewidth=1)
plt.xlabel('age')
plt.ylabel('Proportion of Total')
plt.show()
```

Here 9 bins were used. Rather than using raw counts (the default), the vertical axis here gives the percentage in each class, defined by $\frac{\text{count}}{\text{total}}$. This is achieved by choosing the "weights" parameter to be equal to the vector with entries $1/266$, with length 226. Various plotting parameters have also been changed.

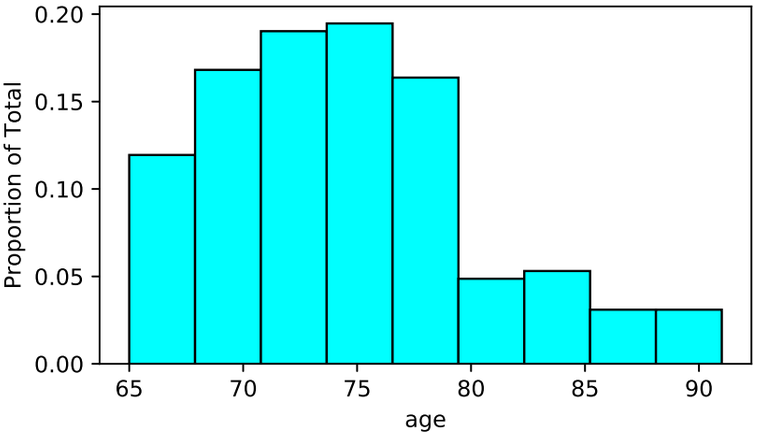


Figure 1.3: Histogram of `'age'`.

Histograms can also be used for discrete features, although it may be necessary to explicitly specify the bins and placement of the ticks on the axes.

1.5.2.3 Empirical Cumulative Distribution Function

EMPIRICAL CUMULATIVE DISTRIBUTION FUNCTION

The *empirical cumulative distribution function*, denoted by F_n, is a step function which jumps an amount k/n at observation values, where k is the number of tied observations at that value. For observations $x_1, \ldots, x_n$, $F_n(x)$ is the fraction of observations less than or equal to x, i.e.,

$$F_n(x) = \frac{\text{number of } x_i \leqslant x}{n} = \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}\{x_i \leqslant x\}, \tag{1.2}$$

INDICATOR

where $\mathbb{1}$ denotes the *indicator* function; that is, $\mathbb{1}\{x_i \leqslant x\}$ is equal to 1 when $x_i \leqslant x$ and 0 otherwise. To produce a plot of the empirical cumulative distribution function we can use the **`plt.step`** function. The result for the age data is shown in Figure 1.4. The empirical cumulative distribution function for a discrete quantitative variable is obtained in the same way.

```
x = np.sort(nutri.age)
y = np.linspace(0,1,len(nutri.age))
plt.xlabel('age')
plt.ylabel('Fn(x)')
plt.step(x,y)
plt.xlim(x.min(),x.max())
plt.show()
```

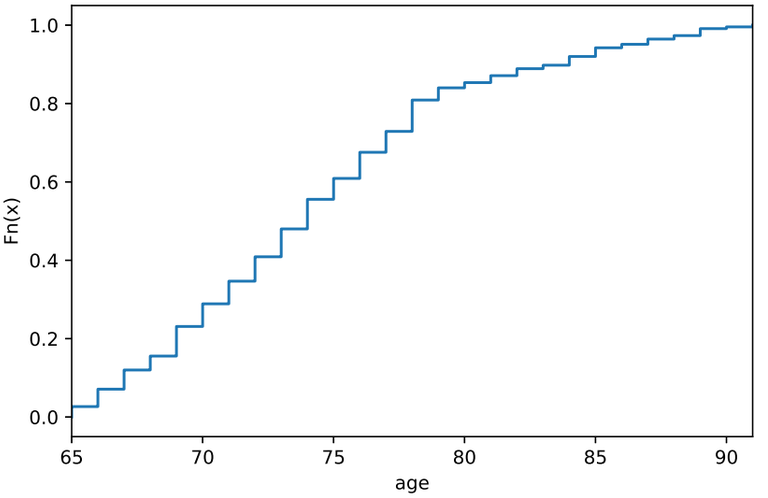


Figure 1.4: Plot of the empirical distribution function for the continuous quantitative feature `'age'`.

1.5.3 Data Visualization in a Bivariate Setting

In this section, we present a few useful visual aids to explore relationships between two features. The graphical representation will depend on the type of the two features.

1.5.3.1 Two-way Plots for Two Categorical Variables

Comparing barplots for two categorical variables involves introducing subplots to the figure. Figure 1.5 visualizes the contingency table of Section 1.3, which cross-tabulates the family status (situation) with the gender of the elderly people. It simply shows two barplots next to each other in the same figure.

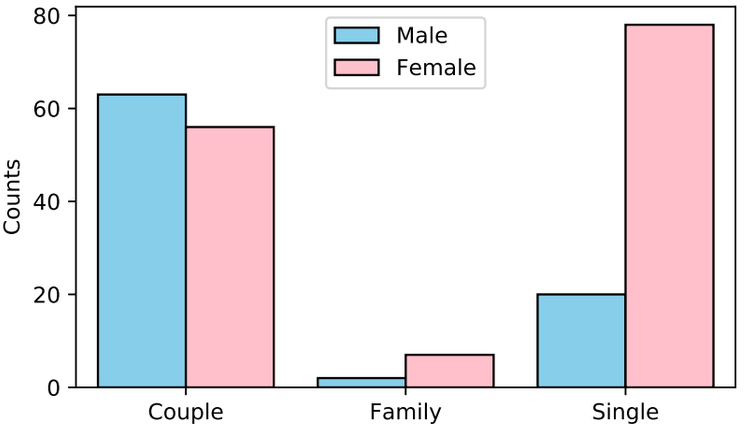


Figure 1.5: Barplot for two categorical variables.

The figure was made using the **seaborn** package, which was specifically designed to simplify statistical visualization tasks.

```
import seaborn as sns
sns.countplot(x='situation', hue = 'gender', data=nutri,
     hue_order = ['Male', 'Female'], palette = ['SkyBlue','Pink'],
      saturation = 1, edgecolor='black')
plt.legend(loc='upper center')
plt.xlabel('')
plt.ylabel('Counts')
plt.show()
```

1.5.3.2 Plots for Two Quantitative Variables

We can visualize patterns between two quantitative features using a *scatterplot*. This can be done with `plt.scatter`. The following code produces a scatterplot of `'weight'` against `'height'` for the `nutri` data.

SCATTERPLOT

```
plt.scatter(nutri.height, nutri.weight, s=12, marker='o')
plt.xlabel('height')
plt.ylabel('weight')
plt.show()
```

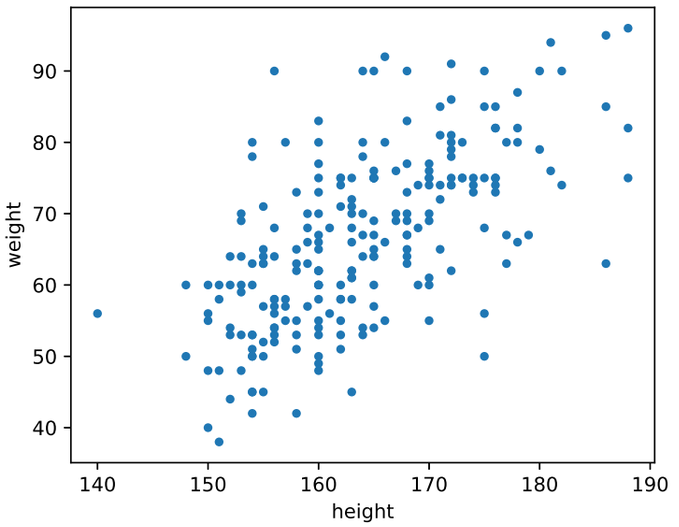


Figure 1.6: Scatterplot of `'weight'` against `'height'`.

The next Python code illustrates that it is possible to produce highly sophisticated scatter plots, such as in Figure 1.7. The figure shows the birth weights (mass) of babies whose mothers smoked (blue triangles) or not (red circles). In addition, straight lines were fitted to the two groups, suggesting that birth weight decreases with age when the mother smokes, but increases when the mother does not smoke! The question is whether these trends are statistically significant or due to chance. We will revisit this data set later on in the book.

☞ 199

```
urlprefix = 'https://vincentarelbundock.github.io/Rdatasets/csv/'
dataname = 'MASS/birthwt.csv'
bwt = pd.read_csv(urlprefix + dataname)
bwt = bwt.drop('Unnamed: 0',1)   #drop unnamed column
styles = {0: ['o','red'], 1: ['^','blue']}
for k in styles:
    grp = bwt[bwt.smoke==k]
    m,b = np.polyfit(grp.age, grp.bwt, 1) # fit a straight line
    plt.scatter(grp.age, grp.bwt, c=styles[k][1], s=15, linewidth=0,
        marker = styles[k][0])
    plt.plot(grp.age, m*grp.age + b, '-', color=styles[k][1])

plt.xlabel('age')
plt.ylabel('birth weight (g)')
plt.legend(['non-smokers','smokers'],prop={'size':8},
            loc=(0.5,0.8))
plt.show()
```

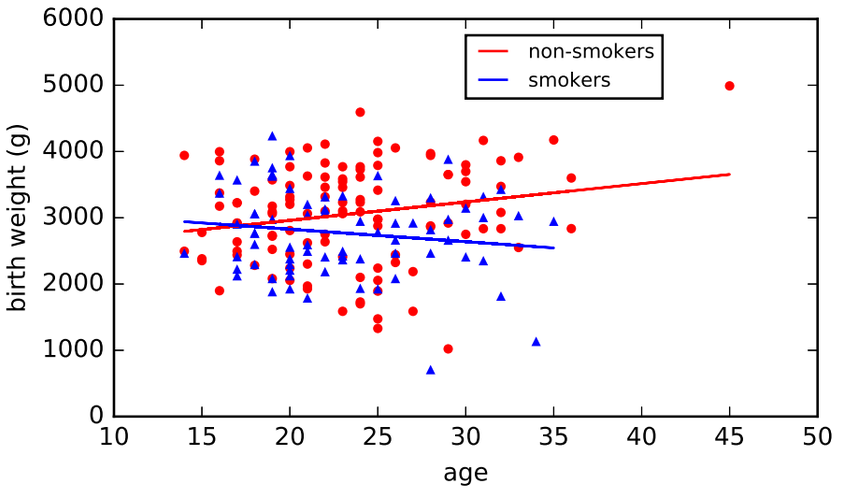


Figure 1.7: Birth weight against age for smoking and non-smoking mothers.

1.5.3.3 Plots for One Qualitative and One Quantitative Variable

In this setting, it is interesting to draw boxplots of the quantitative feature for each level of the categorical feature. Assuming the variables are structured correctly, the function **plt.boxplot** can be used to produce Figure 1.8, using the following code:

```
males = nutri[nutri.gender == 'Male']
females = nutri[nutri.gender == 'Female']
plt.boxplot([males.coffee,females.coffee],notch=True,widths
    =(0.5,0.5))
plt.xlabel('gender')
plt.ylabel('coffee')
plt.xticks([1,2],['Male','Female'])
plt.show()
```

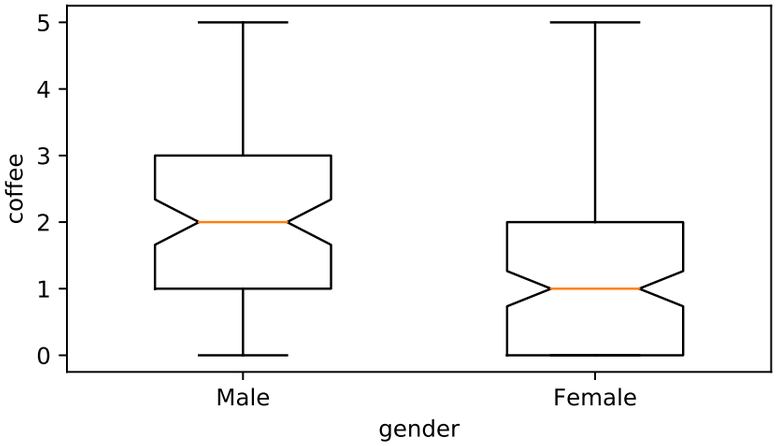


Figure 1.8: Boxplots of a quantitative feature `'coffee'` as a function of the levels of a categorical feature `'gender'`. Note that we used a different, "notched", style boxplot this time.

Further Reading

The focus in this book is on the mathematical and statistical analysis of data, and for the rest of the book we assume that the data is available in a suitable form for analysis. However, a large part of practical data science involves the *cleaning* of data; that is, putting it into a form that is amenable to analysis with standard software packages. Standard Python modules such as **numpy** and **pandas** can be used to reformat rows, rename columns, remove faulty outliers, merge rows, and so on. McKinney, the creator of **pandas**, gives many practical case studies in [84]. Effective data visualization techniques are beautifully illustrated in [65].

Exercises

Before you attempt these exercises, make sure you have up-to-date versions of the relevant Python packages, specifically **matplotlib**, **pandas**, and **seaborn**. An easy way to ensure this is to update packages via the Anaconda Navigator, as explained in Appendix D.

1. Visit the UCI Repository https://archive.ics.uci.edu/. Read the description of the data and download the Mushroom data set `agaricus-lepiota.data`. Using **pandas**, read the data into a `DataFrame` called `mushroom`, via **read_csv**.

   (a) How many features are in this data set?

   (b) What are the initial names and types of the features?

   (c) Rename the first feature (index 0) to `'edibility'` and the sixth feature (index 5) to `'odor'` [Hint: the column names in **pandas** are immutable; so individual columns cannot be modified directly. However it is possible to assign the entire column names list via `mushroom.columns = newcols`.]

(d) The 6th column lists the various odors of the mushrooms: encoded as `'a'`, `'c'`, ... Replace these with the names `'almond'`, `'creosote'`, etc. (categories corresponding to each letter can be found on the website). Also replace the `'edibility'` categories `'e'` and `'p'` with `'edible'` and `'poisonous'`.

(e) Make a contingency table cross-tabulating `'edibility'` and `'odor'`.

(f) Which mushroom odors should be avoided, when gathering mushrooms for consumption?

(g) What proportion of odorless mushroom samples were safe to eat?

2. Change the type and value of variables in the **nutri** data set according to Table 1.2 and save the data as a CSV file. The modified data should have eight categorical features, three floats, and two integer features.

3. It frequently happens that a table with data needs to be restructured before the data can be analyzed using standard statistical software. As an example, consider the test scores in Table 1.3 of 5 students before and after specialized tuition.

Table 1.3: Student scores.

Student	Before	After
1	75	85
2	30	50
3	100	100
4	50	52
5	60	65

This is not in the standard format described in Section 1.1. In particular, the student scores are divided over two columns, whereas the standard format requires that they are collected in one column, e.g., labelled `'Score'`. Reformat (by hand) the table in standard format, using three features:

- `'Score'`, taking continuous values,
- `'Time'`, taking values `'Before'` and `'After'`,
- `'Student'`, taking values from 1 to 5.

Useful methods for reshaping tables in **pandas** are **melt**, **stack**, and **unstack**.

4. Create a similar barplot as in Figure 1.5, but now plot the corresponding *proportions* of males and females in each of the three situation categories. That is, the heights of the bars should sum up to 1 for both barplots with the same `'gender'` value. [Hint: **seaborn** does not have this functionality built in, instead you need to first create a contingency table and use **matplotlib.pyplot** to produce the figure.]

☞ 2

5. The **iris** data set, mentioned in Section 1.1, contains various features, including `'Petal.Length'` and `'Sepal.Length'`, of three species of iris: setosa, versicolor, and virginica.

(a) Load the data set into a **pandas** `DataFrame` object.

(b) Using **matplotlib.pyplot**, produce boxplots of `'Petal.Length'` for each the three species, in one figure.

(c) Make a histogram with 20 bins for `'Petal.Length'`.

(d) Produce a similar scatterplot for `'Sepal.Length'` against `'Petal.Length'` to that of the left plot in Figure 1.9. Note that the points should be colored according to the `'Species'` feature as per the legend in the right plot of the figure.

(e) Using the **kdeplot** method of the **seaborn** package, reproduce the right plot of Figure 1.9, where kernel density plots for `'Petal.Length'` are given. ☞ 131

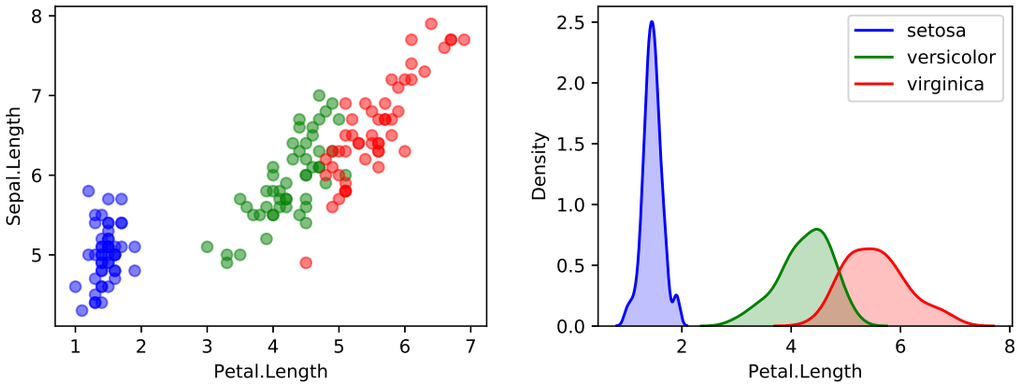


Figure 1.9: Left: scatterplot of `'Sepal.Length'` against `'Petal.Length'`. Right: kernel density estimates of `'Petal.Length'` for the three species of iris.

6. Import the data set **EuStockMarkets** from the same website as the **iris** data set above. The data set contains the daily closing prices of four European stock indices during the 1990s, for 260 working days per year.

(a) Create a vector of times (working days) for the stock prices, between 1991.496 and 1998.646 with increments of 1/260.

(b) Reproduce Figure 1.10. [Hint: Use a dictionary to map column names (stock indices) to colors.]

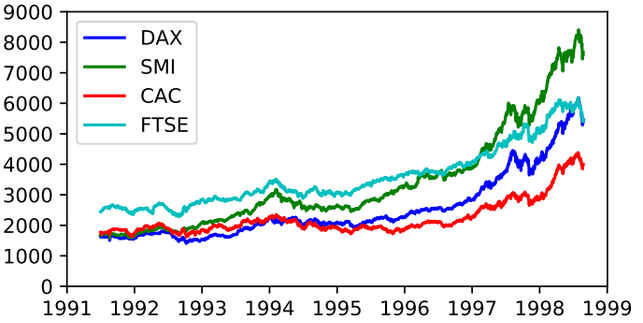


Figure 1.10: Closing stock indices for various European stock markets.

7. Consider the KASANDR data set from the UCI Machine Learning Repository, which can be downloaded from

https://archive.ics.uci.edu/ml/machine-learning-databases/00385/de.tar.bz2.

This archive file has a size of 900Mb, so it may take a while to download. Uncompressing the file (e.g., via 7-Zip) yields a directory de containing two large CSV files: `test_de.csv` and `train_de.csv`, with sizes 372Mb and 3Gb, respectively. Such large data files can still be processed efficiently in **pandas**, provided there is enough memory. The files contain records of user information from Kelkoo web logs in Germany as well as meta-data on users, offers, and merchants. The data sets have 7 attributes and 1919561 and 15844717 rows, respectively. The data sets are anonymized via hex strings.

(a) Load `train_de.csv` into a **pandas** `DataFrame` object **de**, using

```
read_csv('train_de.csv', delimiter = '\t').
```

If not enough memory is available, load `test_de.csv` instead. Note that entries are separated here by tabs, not commas. Time how long it takes for the file to load, using the **time** package. (It took 38 seconds for `train_de.csv` to load on one of our computers.)

(b) How many unique users and merchants are in this data set?

8. Visualizing data involving more than two features requires careful design, which is often more of an art than a science.

(a) Go to Vincent Arel-Bundocks's website (URL given in Section 1.1) and read the `Orange` data set into a **pandas** `DataFrame object` called **orange**. Remove its first (unnamed) column.

(b) The data set contains the circumferences of 5 orange trees at various stages in their development. Find the names of the features.

(c) In Python, import **seaborn** and visualize the growth curves (circumference against age) of the trees, using the **regplot** and **FacetGrid** methods.

CHAPTER 2

STATISTICAL LEARNING

The purpose of this chapter is to introduce the reader to some common concepts and themes in statistical learning. We discuss the difference between supervised and unsupervised learning, and how we can assess the predictive performance of supervised learning. We also examine the central role that the linear and Gaussian properties play in the modeling of data. We conclude with a section on Bayesian learning. The required probability and statistics background is given in Appendix C.

2.1 Introduction

Although structuring and visualizing data are important aspects of data science, the main challenge lies in the mathematical analysis of the data. When the goal is to interpret the model and quantify the uncertainty in the data, this analysis is usually referred to as *statistical learning*. In contrast, when the emphasis is on making predictions using large-scale data, then it is common to speak about *machine learning* or *data mining*.

STATISTICAL LEARNING

MACHINE LEARNING

DATA MINING

There are two major goals for modeling data: 1) to accurately predict some future quantity of interest, given some observed data, and 2) to discover unusual or interesting patterns in the data. To achieve these goals, one must rely on knowledge from three important pillars of the mathematical sciences.

Function approximation. Building a mathematical model for data usually means understanding how one data variable depends on another data variable. The most natural way to represent the relationship between variables is via a mathematical function or map. We usually assume that this mathematical function is not completely known, but can be approximated well given enough computing power and data. Thus, data scientists have to understand how best to approximate and represent functions using the least amount of computer processing and memory.

Optimization. Given a class of mathematical models, we wish to find the best possible model in that class. This requires some kind of efficient search or optimization procedure. The optimization step can be viewed as a process of fitting or calibrating a function to observed data. This step usually requires knowledge of optimization algorithms and efficient computer coding or programming.

Probability and Statistics. In general, the data used to fit the model is viewed as a realization of a random process or numerical vector, whose probability law determines the accuracy with which we can predict future observations. Thus, in order to quantify the uncertainty inherent in making predictions about the future, and the sources of error in the model, data scientists need a firm grasp of probability theory and statistical inference.

2.2 Supervised and Unsupervised Learning

FEATURE
RESPONSE

Given an input or *feature* vector $\boldsymbol{x}$, one of the main goals of machine learning is to predict an output or *response* variable y. For example, $\boldsymbol{x}$ could be a digitized signature and y a binary variable that indicates whether the signature is genuine or false. Another example is where $\boldsymbol{x}$ represents the weight and smoking habits of an expecting mother and y the birth weight of the baby. The data science attempt at this prediction is encoded in a mathematical function g, called the *prediction function*, which takes as an input $\boldsymbol{x}$ and outputs a guess $g(\boldsymbol{x})$ for y (denoted by $\widehat{y}$, for example). In a sense, g encompasses all the information about the relationship between the variables $\boldsymbol{x}$ and y, excluding the effects of chance and randomness in nature.

PREDICTION FUNCTION

REGRESSION

In *regression* problems, the response variable y can take any real value. In contrast, when y can only lie in a finite set, say $y \in \{0, \ldots, c-1\}$, then predicting y is conceptually the same as classifying the input $\boldsymbol{x}$ into one of c categories, and so prediction becomes a *classification* problem.

CLASSIFICATION

LOSS FUNCTION

We can measure the accuracy of a prediction $\widehat{y}$ with respect to a given response y by using some *loss function* $\text{Loss}(y, \widehat{y})$. In a regression setting the usual choice is the squared-error loss $(y-\widehat{y})^2$. In the case of classification, the zero–one (also written 0–1) loss function $\text{Loss}(y, \widehat{y}) = \mathbb{1}\{y \neq \widehat{y}\}$ is often used, which incurs a loss of 1 whenever the predicted class $\widehat{y}$ is not equal to the class y. Later on in this book, we will encounter various other useful loss functions, such as the cross-entropy and hinge loss functions (see, e.g., Chapter 7).

The word *error* is often used as a measure of distance between a "true" object y and some approximation $\widehat{y}$ thereof. If y is real-valued, the absolute error $|y-\widehat{y}|$ and the squared error $(y-\widehat{y})^2$ are both well-established error concepts, as are the norm $\|\boldsymbol{y}-\widehat{\boldsymbol{y}}\|$ and squared norm $\|\boldsymbol{y}-\widehat{\boldsymbol{y}}\|^2$ for vectors. The squared error $(y-\widehat{y})^2$ is just one example of a loss function.

It is unlikely that any mathematical function g will be able to make accurate predictions for all possible pairs $(\boldsymbol{x}, y)$ one may encounter in Nature. One reason for this is that, even with the same input $\boldsymbol{x}$, the output y may be different, depending on chance circumstances or randomness. For this reason, we adopt a probabilistic approach and assume that each pair $(\boldsymbol{x}, y)$ is the outcome of a random pair $(\boldsymbol{X}, Y)$ that has some joint probability density $f(\boldsymbol{x}, y)$. We then assess the predictive performance via the expected loss, usually called the *risk*, for g:

RISK

$$\ell(g) = \mathbb{E}\,\text{Loss}(Y, g(\boldsymbol{X})). \tag{2.1}$$

For example, in the classification case with zero–one loss function the risk is equal to the probability of incorrect classification: $\ell(g) = \mathbb{P}[Y \neq g(\boldsymbol{X})]$. In this context, the prediction

function g is called a *classifier*. Given the distribution of $(\boldsymbol{X}, Y)$ and any loss function, we can in principle find the best possible $g^* := \operatorname{argmin}_g \mathbb{E}\,\mathrm{Loss}(Y, g(\boldsymbol{X}))$ that yields the smallest risk $\ell^* := \ell(g^*)$. We will see in Chapter 7 that in the classification case with $y \in \{0, \ldots, c-1\}$ and $\ell(g) = \mathbb{P}[Y \neq g(\boldsymbol{X})]$, we have

CLASSIFIER

☞ 253

$$g^*(\boldsymbol{x}) = \operatorname*{argmax}_{y \in \{0,\ldots,c-1\}} f(y \,|\, \boldsymbol{x}),$$

where $f(y \,|\, \boldsymbol{x}) = \mathbb{P}[Y = y \,|\, \boldsymbol{X} = \boldsymbol{x}]$ is the conditional probability of $Y = y$ given $\boldsymbol{X} = \boldsymbol{x}$. As already mentioned, for regression the most widely-used loss function is the squared-error loss. In this setting, the optimal prediction function g^* is often called the *regression function*. The following theorem specifies its exact form.

REGRESSION FUNCTION

Theorem 2.1: Optimal Prediction Function for Squared-Error Loss

For the squared-error loss $\mathrm{Loss}(y, \widehat{y}) = (y - \widehat{y})^2$, the optimal prediction function g^* is equal to the conditional expectation of Y given $\boldsymbol{X} = \boldsymbol{x}$:

$$g^*(\boldsymbol{x}) = \mathbb{E}[Y \,|\, \boldsymbol{X} = \boldsymbol{x}].$$

Proof: Let $g^*(\boldsymbol{x}) = \mathbb{E}[Y \,|\, \boldsymbol{X} = \boldsymbol{x}]$. For any function g, the squared-error risk satisfies

$$\begin{aligned}
\mathbb{E}(Y - g(\boldsymbol{X}))^2 &= \mathbb{E}[(Y - g^*(\boldsymbol{X}) + g^*(\boldsymbol{X}) - g(\boldsymbol{X}))^2] \\
&= \mathbb{E}(Y - g^*(\boldsymbol{X}))^2 + 2\mathbb{E}[(Y - g^*(\boldsymbol{X}))(g^*(\boldsymbol{X}) - g(\boldsymbol{X}))] + \mathbb{E}(g^*(\boldsymbol{X}) - g(\boldsymbol{X}))^2 \\
&\geqslant \mathbb{E}(Y - g^*(\boldsymbol{X}))^2 + 2\mathbb{E}[(Y - g^*(\boldsymbol{X}))(g^*(\boldsymbol{X}) - g(\boldsymbol{X}))] \\
&= \mathbb{E}(Y - g^*(\boldsymbol{X}))^2 + 2\mathbb{E}\left\{(g^*(\boldsymbol{X}) - g(\boldsymbol{X}))\mathbb{E}[Y - g^*(\boldsymbol{X}) \,|\, \boldsymbol{X}]\right\}.
\end{aligned}$$

In the last equation we used the tower property. By the definition of the conditional expectation, we have $\mathbb{E}[Y - g^*(\boldsymbol{X}) \,|\, \boldsymbol{X}] = 0$. It follows that $\mathbb{E}(Y - g(\boldsymbol{X}))^2 \geqslant \mathbb{E}(Y - g^*(\boldsymbol{X}))^2$, showing that g^* yields the smallest squared-error risk. □

☞ 433

One consequence of Theorem 2.1 is that, conditional on $\boldsymbol{X} = \boldsymbol{x}$, the (random) response Y can be written as

$$Y = g^*(\boldsymbol{x}) + \varepsilon(\boldsymbol{x}), \tag{2.2}$$

where $\varepsilon(\boldsymbol{x})$ can be viewed as the random deviation of the response from its conditional mean at $\boldsymbol{x}$. This random deviation satisfies $\mathbb{E}\,\varepsilon(\boldsymbol{x}) = 0$. Further, the conditional variance of the response Y at $\boldsymbol{x}$ can be written as $\mathbb{V}\mathrm{ar}\,\varepsilon(\boldsymbol{x}) = v^2(\boldsymbol{x})$ for some unknown positive function v. Note that, in general, the probability distribution of $\varepsilon(\boldsymbol{x})$ is unspecified.

Since, the optimal prediction function g^* depends on the typically unknown joint distribution of $(\boldsymbol{X}, Y)$, it is not available in practice. Instead, all that we have available is a finite number of (usually) independent realizations from the joint density $f(\boldsymbol{x}, y)$. We denote this sample by $\mathcal{T} = \{(\boldsymbol{X}_1, Y_1), \ldots, (\boldsymbol{X}_n, Y_n)\}$ and call it the *training set* ($\mathcal{T}$ is a mnemonic for training) with n examples. It will be important to distinguish between a random training set $\mathcal{T}$ and its (deterministic) outcome $\{(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)\}$. We will use the notation τ for the latter. We will also add the subscript n in τ_n when we wish to emphasize the size of the training set.

TRAINING SET

Our goal is thus to "learn" the unknown g^* using the n examples in the training set $\mathcal{T}$. Let us denote by $g_{\mathcal{T}}$ the best (by some criterion) approximation for g^* that we can construct

from $\mathcal{T}$. Note that $g_{\mathcal{T}}$ is a random function. A particular outcome is denoted by g_τ. It is often useful to think of a teacher–learner metaphor, whereby the function $g_{\mathcal{T}}$ is a *learner* who learns the unknown functional relationship $g^* : \boldsymbol{x} \mapsto y$ from the training data $\mathcal{T}$. We can imagine a "teacher" who provides n examples of the true relationship between the output Y_i and the input $\boldsymbol{X}_i$ for $i = 1, \ldots, n$, and thus "trains" the learner $g_{\mathcal{T}}$ to predict the output of a new input $\boldsymbol{X}$, for which the correct output Y is not provided by the teacher (is unknown).

LEARNER

SUPERVISED LEARNING

The above setting is called *supervised learning*, because one tries to learn the functional relationship between the feature vector $\boldsymbol{x}$ and response y in the presence of a teacher who provides n examples. It is common to speak of "explaining" or predicting y on the basis of $\boldsymbol{x}$, where $\boldsymbol{x}$ is a vector of *explanatory variables*.

EXPLANATORY VARIABLES

An example of supervised learning is email spam detection. The goal is to train the learner $g_{\mathcal{T}}$ to accurately predict whether any future email, as represented by the feature vector $\boldsymbol{x}$, is spam or not. The training data consists of the feature vectors of a number of different email examples as well as the corresponding labels (spam or not spam). For instance, a feature vector could consist of the number of times sales-pitch words like "free", "sale", or "miss out" occur within a given email.

As seen from the above discussion, most questions of interest in supervised learning can be answered if we know the conditional pdf $f(y \mid \boldsymbol{x})$, because we can then in principle work out the function value $g^*(\boldsymbol{x})$.

UNSUPERVISED LEARNING

In contrast, *unsupervised learning* makes no distinction between response and explanatory variables, and the objective is simply to learn the structure of the unknown distribution of the data. In other words, we need to learn $f(\boldsymbol{x})$. In this case the guess $g(\boldsymbol{x})$ is an approximation of $f(\boldsymbol{x})$ and the risk is of the form

$$\ell(g) = \mathbb{E}\,\mathrm{Loss}(f(\boldsymbol{X}), g(\boldsymbol{X})).$$

An example of unsupervised learning is when we wish to analyze the purchasing behaviors of the customers of a grocery shop that has a total of, say, a hundred items on sale. A feature vector here could be a binary vector $\boldsymbol{x} \in \{0,1\}^{100}$ representing the items bought by a customer on a visit to the shop (a 1 in the k-th position if a customer bought item $k \in \{1, \ldots, 100\}$ and a 0 otherwise). Based on a training set $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, we wish to find any interesting or unusual purchasing patterns. In general, it is difficult to know if an unsupervised learner is doing a good job, because there is no teacher to provide examples of accurate predictions.

The main methodologies for unsupervised learning include *clustering*, *principal component analysis*, and *kernel density estimation*, which will be discussed in Chapter 4.

☞ 121

In the next three sections we will focus on supervised learning. The main supervised learning methodologies are *regression* and *classification*, to be discussed in detail in Chapters 5 and 7. More advanced supervised learning techniques, including *reproducing kernel Hilbert spaces*, *tree methods*, and *deep learning*, will be discussed in Chapters 6, 8, and 9.

☞ 167
☞ 253

2.3 Training and Test Loss

Given an arbitrary prediction function g, it is typically not possible to compute its risk $\ell(g)$ in (2.1). However, using the training sample $\mathcal{T}$, we can approximate $\ell(g)$ via the empirical (sample average) risk

$$\ell_{\mathcal{T}}(g) = \frac{1}{n}\sum_{i=1}^{n} \text{Loss}(Y_i, g(\boldsymbol{X}_i)), \tag{2.3}$$

which we call the *training loss*. The training loss is thus an unbiased estimator of the risk (the expected loss) for a prediction function g, based on the training data. TRAINING LOSS

To approximate the optimal prediction function g^* (the minimizer of the risk $\ell(g)$) we first select a suitable collection of approximating functions $\mathcal{G}$ and then take our *learner* to be the function in $\mathcal{G}$ that minimizes the training loss; that is,

$$g_{\mathcal{T}}^{\mathcal{G}} = \operatorname*{argmin}_{g\in\mathcal{G}} \ell_{\mathcal{T}}(g). \tag{2.4}$$

For example, the simplest and most useful $\mathcal{G}$ is the set of *linear* functions of $\boldsymbol{x}$; that is, the set of all functions $g : \boldsymbol{x} \mapsto \boldsymbol{\beta}^\top \boldsymbol{x}$ for some real-valued vector $\boldsymbol{\beta}$.

We suppress the superscript $\mathcal{G}$ when it is clear which function class is used. Note that minimizing the training loss over all possible functions g (rather than over all $g \in \mathcal{G}$) does not lead to a meaningful optimization problem, as any function g for which $g(\boldsymbol{X}_i) = Y_i$ for all i gives minimal training loss. In particular, for a squared-error loss, the training loss will be 0. Unfortunately, such functions have a poor ability to predict new (that is, independent from $\mathcal{T}$) pairs of data. This poor generalization performance is called *overfitting*. OVERFITTING

By choosing g a function that predicts the training data exactly (and is, for example, 0 otherwise), the squared-error training loss is zero. Minimizing the training loss is not the ultimate goal!

The prediction accuracy of new pairs of data is measured by the *generalization risk* of the learner. For a *fixed* training set τ it is defined as GENERALIZATION RISK

$$\ell(g_\tau^{\mathcal{G}}) = \mathbb{E}\,\text{Loss}(Y, g_\tau^{\mathcal{G}}(\boldsymbol{X})), \tag{2.5}$$

where $(\boldsymbol{X}, Y)$ is distributed according to $f(\boldsymbol{x}, y)$. In the discrete case the generalization risk is therefore: $\ell(g_\tau^{\mathcal{G}}) = \sum_{\boldsymbol{x},y} \text{Loss}(y, g_\tau^{\mathcal{G}}(\boldsymbol{x}))f(\boldsymbol{x}, y)$ (replace the sum with an integral for the continuous case). The situation is illustrated in Figure 2.1, where the distribution of $(\boldsymbol{X}, Y)$ is indicated by the red dots. The training set (points in the shaded regions) determines a fixed prediction function shown as a straight line. Three possible outcomes of $(\boldsymbol{X}, Y)$ are shown (black dots). The amount of loss for each point is shown as the length of the dashed lines. The generalization risk is the average loss over all possible pairs $(\boldsymbol{x}, y)$, weighted by the corresponding $f(\boldsymbol{x}, y)$.

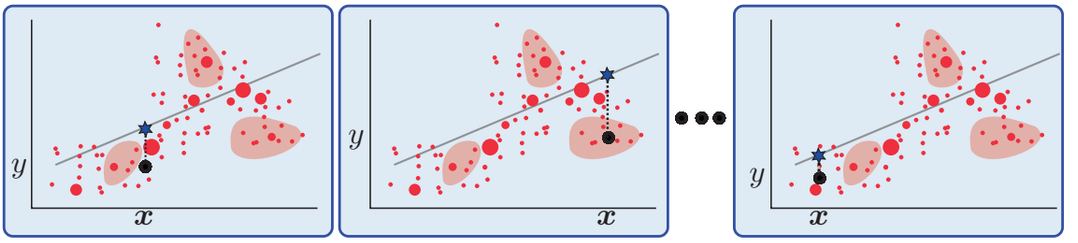


Figure 2.1: The generalization risk for a fixed training set is the weighted-average loss over all possible pairs $(\boldsymbol{x}, y)$.

For a *random* training set $\mathcal{T}$, the generalization risk is thus a random variable that depends on $\mathcal{T}$ (and $\mathcal{G}$). If we average the generalization risk over all possible instances of $\mathcal{T}$, we obtain the *expected generalization risk*:

EXPECTED GENERALIZATION RISK

$$\mathbb{E}\,\ell(g_{\mathcal{T}}^{\mathcal{G}}) = \mathbb{E}\,\mathrm{Loss}(Y, g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{X})), \tag{2.6}$$

where $(\boldsymbol{X}, Y)$ in the expectation above is independent of $\mathcal{T}$. In the discrete case, we have $\mathbb{E}\ell(g_{\mathcal{T}}^{\mathcal{G}}) = \sum_{\boldsymbol{x},y,\boldsymbol{x}_1,y_1,\ldots,\boldsymbol{x}_n,y_n} \mathrm{Loss}(y, g_{\tau}^{\mathcal{G}}(\boldsymbol{x}))f(\boldsymbol{x}, y)f(\boldsymbol{x}_1, y_1)\cdots f(\boldsymbol{x}_n, y_n)$. Figure 2.2 gives an illustration.

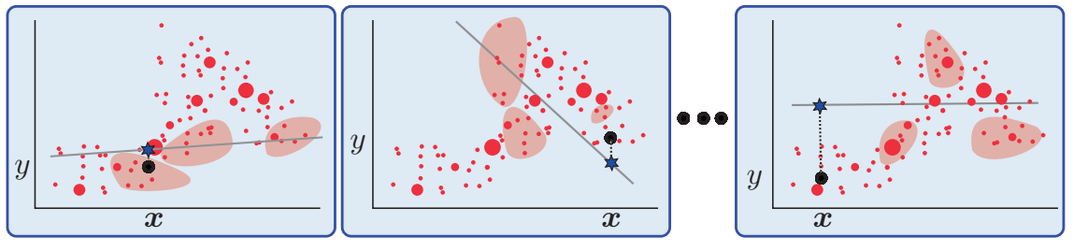


Figure 2.2: The expected generalization risk is the weighted-average loss over all possible pairs $(\boldsymbol{x}, y)$ and over all training sets.

For any outcome τ of the training data, we can estimate the generalization risk without bias by taking the sample average

$$\ell_{\mathcal{T}'}(g_{\tau}^{\mathcal{G}}) := \frac{1}{n'}\sum_{i=1}^{n'} \mathrm{Loss}(Y_i', g_{\tau}^{\mathcal{G}}(\boldsymbol{X}_i')), \tag{2.7}$$

TEST SAMPLE

TEST LOSS

where $\{(\boldsymbol{X}_1', Y_1'), \ldots, (\boldsymbol{X}_{n'}', Y_{n'}')\} =: \mathcal{T}'$ is a so-called *test sample*. The test sample is completely separate from $\mathcal{T}$, but is drawn in the same way as $\mathcal{T}$; that is, via independent draws from $f(\boldsymbol{x}, y)$, for some sample size n'. We call the estimator (2.7) the *test loss*. For a random training set $\mathcal{T}$ we can define $\ell_{\mathcal{T}'}(g_{\mathcal{T}}^{\mathcal{G}})$ similarly. It is then crucial to assume that $\mathcal{T}$ is independent of $\mathcal{T}'$. Table 2.1 summarizes the main definitions and notation for supervised learning.

Table 2.1: Summary of definitions for supervised learning.

$\boldsymbol{x}$	Fixed explanatory (feature) vector.
$\boldsymbol{X}$	Random explanatory (feature) vector.
y	Fixed (real-valued) response.
Y	Random response.
$f(\boldsymbol{x}, y)$	Joint pdf of $\boldsymbol{X}$ and Y, evaluated at $(\boldsymbol{x}, y)$.
$f(y \mid \boldsymbol{x})$	Conditional pdf of Y given $\boldsymbol{X} = \boldsymbol{x}$, evaluated at y.
τ or τ_n	Fixed training data $\{(\boldsymbol{x}_i, y_i), i = 1, \ldots, n\}$.
$\mathcal{T}$ or $\mathcal{T}_n$	Random training data $\{(\boldsymbol{X}_i, Y_i), i = 1, \ldots, n\}$.
$\mathbf{X}$	Matrix of explanatory variables, with n rows $\boldsymbol{x}_i^\top, i = 1, \ldots, n$ and $\dim(\boldsymbol{x})$ feature columns; one of the features may be the constant 1.
$\boldsymbol{y}$	Vector of response variables $(y_1, \ldots, y_n)^\top$.
g	Prediction (guess) function.
$\text{Loss}(y, \widehat{y})$	Loss incurred when predicting response y with $\widehat{y}$.
$\ell(g)$	Risk for prediction function g; that is, $\mathbb{E}\,\text{Loss}(Y, g(\boldsymbol{X}))$.
g^*	Optimal prediction function; that is, $\operatorname{argmin}_g \ell(g)$.
$g^{\mathcal{G}}$	Optimal prediction function in function class $\mathcal{G}$; that is, $\operatorname{argmin}_{g \in \mathcal{G}} \ell(g)$.
$\ell_\tau(g)$	Training loss for prediction function g; that is, the sample average estimate of $\ell(g)$ based on a fixed training sample τ.
$\ell_{\mathcal{T}}(g)$	The same as $\ell_\tau(g)$, but now for a random training sample $\mathcal{T}$.
$g_\tau^{\mathcal{G}}$ or g_τ	The *learner*: $\operatorname{argmin}_{g \in \mathcal{G}} \ell_\tau(g)$. That is, the optimal prediction function based on a fixed training set τ and function class $\mathcal{G}$. We suppress the superscript $\mathcal{G}$ if the function class is implicit.
$g_{\mathcal{T}}^{\mathcal{G}}$ or $g_{\mathcal{T}}$	The learner, where we have replaced τ with a random training set $\mathcal{T}$.

To compare the predictive performance of various learners in the function class $\mathcal{G}$, as measured by the test loss, we can use the *same* fixed training set τ and test set τ' for all learners. When there is an abundance of data, the "overall" data set is usually (randomly) divided into a training and test set, as depicted in Figure 2.3. We then use the training data to construct various learners $g_\tau^{\mathcal{G}_1}, g_\tau^{\mathcal{G}_2}, \ldots$, and use the test data to select the best (with the smallest test loss) among these learners. In this context the test set is called the *validation set*. Once the best learner has been chosen, a third "test" set can be used to assess the predictive performance of the best learner. The training, validation, and test sets can again be obtained from the overall data set via a random allocation. When the overall data set is of modest size, it is customary to perform the validation phase (model selection) on the training set only, using cross-validation. This is the topic of Section 2.5.2.

VALIDATION SET

☞ 37

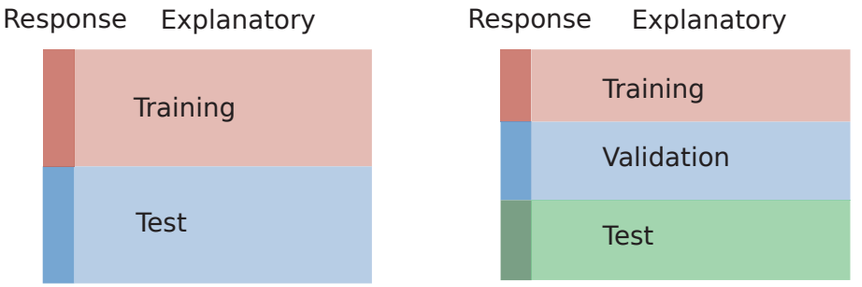


Figure 2.3: Statistical learning algorithms often require the data to be divided into training and test data. If the latter is used for model selection, a third set is needed for testing the performance of the selected model.

We next consider a concrete example that illustrates the concepts introduced so far.

■ **Example 2.1 (Polynomial Regression)** In what follows, it will appear that we have arbitrarily replaced the symbols $\boldsymbol{x}, g, \mathcal{G}$ with $u, h, \mathcal{H}$, respectively. The reason for this switch of notation will become clear at the end of the example.

The data (depicted as dots) in Figure 2.4 are $n = 100$ points $(u_i, y_i), i = 1, \ldots, n$ drawn from iid random points $(U_i, Y_i), i = 1, \ldots, n$, where the $\{U_i\}$ are uniformly distributed on the interval $(0, 1)$ and, given $U_i = u_i$, the random variable Y_i has a normal distribution with expectation $10 - 140u_i + 400u_i^2 - 250u_i^3$ and variance $\ell^* = 25$. This is an example of a *polynomial regression model*. Using a squared-error loss, the optimal prediction function $h^*(u) = \mathbb{E}[Y \mid U = u]$ is thus

POLYNOMIAL REGRESSION MODEL

$$h^*(u) = 10 - 140u + 400u^2 - 250u^3,$$

which is depicted by the dashed curve in Figure 2.4.

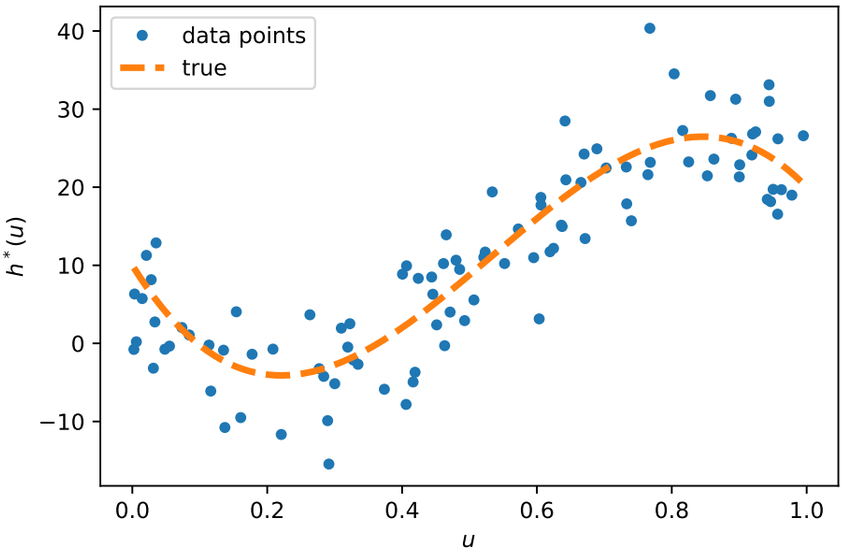


Figure 2.4: Training data and the optimal polynomial prediction function h^*.

To obtain a good estimate of $h^*(u)$ based on the training set $\tau = \{(u_i, y_i), i = 1, \ldots, n\}$, we minimize the outcome of the training loss (2.3):

$$\ell_\tau(h) = \frac{1}{n}\sum_{i=1}^{n}(y_i - h(u_i))^2, \tag{2.8}$$

over a suitable set $\mathcal{H}$ of candidate functions. Let us take the set $\mathcal{H}_p$ of polynomial functions in u of order $p-1$:

$$h(u) := \beta_1 + \beta_2 u + \beta_3 u^2 + \cdots + \beta_p u^{p-1} \tag{2.9}$$

for $p = 1, 2, \ldots$ and parameter vector $\boldsymbol{\beta} = [\beta_1, \beta_2, \ldots, \beta_p]^\top$. This function class contains the best possible $h^*(u) = \mathbb{E}[Y \mid U = u]$ for $p \geqslant 4$. Note that optimization over $\mathcal{H}_p$ is a parametric optimization problem, in that we need to find the best $\boldsymbol{\beta}$. Optimization of (2.8) over $\mathcal{H}_p$ is not straightforward, unless we notice that (2.9) is a *linear* function in $\boldsymbol{\beta}$. In particular, if we map each feature u to a feature vector $\boldsymbol{x} = [1, u, u^2, \ldots, u^{p-1}]^\top$, then the right-hand side of (2.9) can be written as the function

$$g(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta},$$

which is linear in $\boldsymbol{x}$ (as well as $\boldsymbol{\beta}$). The optimal $h^*(u)$ in $\mathcal{H}_p$ for $p \geqslant 4$ then corresponds to the function $g^*(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta}^*$ in the set $\mathcal{G}_p$ of linear functions from $\mathbb{R}^p$ to $\mathbb{R}$, where $\boldsymbol{\beta}^* = [10, -140, 400, -250, 0, \ldots, 0]^\top$. Thus, instead of working with the set $\mathcal{H}_p$ of polynomial functions we may prefer to work with the set $\mathcal{G}_p$ of linear functions. This brings us to a very important idea in statistical learning:

Expand the feature space to obtain a *linear* prediction function.

Let us now reformulate the learning problem in terms of the new explanatory (feature) variables $\boldsymbol{x}_i = [1, u_i, u_i^2, \ldots, u_i^{p-1}]^\top$, $i = 1, \ldots, n$. It will be convenient to arrange these feature vectors into a matrix $\mathbf{X}$ with rows $\boldsymbol{x}_1^\top, \ldots, \boldsymbol{x}_n^\top$:

$$\mathbf{X} = \begin{bmatrix} 1 & u_1 & u_1^2 & \cdots & u_1^{p-1} \\ 1 & u_2 & u_2^2 & \cdots & u_2^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & u_n & u_n^2 & \cdots & u_n^{p-1} \end{bmatrix}. \tag{2.10}$$

Collecting the responses $\{y_i\}$ into a column vector $\boldsymbol{y}$, the training loss (2.3) can now be written compactly as

$$\frac{1}{n}\|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2. \tag{2.11}$$

To find the optimal learner (2.4) in the class $\mathcal{G}_p$ we need to find the minimizer of (2.11):

$$\widehat{\boldsymbol{\beta}} = \operatorname*{argmin}_{\boldsymbol{\beta}} \|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2, \tag{2.12}$$

which is called the *ordinary least-squares* solution. As is illustrated in Figure 2.5, to find $\widehat{\boldsymbol{\beta}}$, we choose $\mathbf{X}\widehat{\boldsymbol{\beta}}$ to be equal to the orthogonal projection of $\boldsymbol{y}$ onto the linear space spanned by the columns of the matrix $\mathbf{X}$; that is, $\mathbf{X}\widehat{\boldsymbol{\beta}} = \mathbf{P}\boldsymbol{y}$, where $\mathbf{P}$ is the *projection matrix*.

ORDINARY LEAST-SQUARES

PROJECTION MATRIX

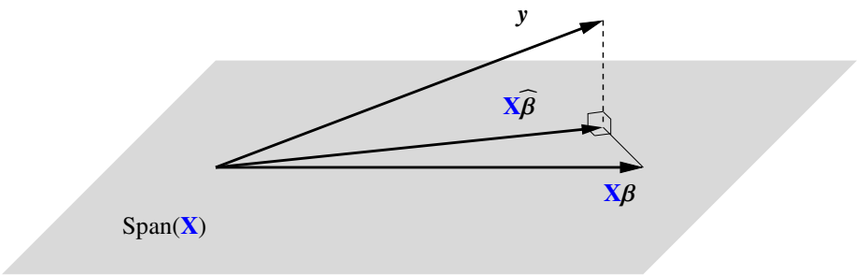


Figure 2.5: $\mathbf{X}\widehat{\boldsymbol{\beta}}$ is the orthogonal projection of $\boldsymbol{y}$ onto the linear space spanned by the columns of the matrix $\mathbf{X}$.

☞ 364

According to Theorem A.4, the projection matrix is given by

$$\mathbf{P} = \mathbf{X}\,\mathbf{X}^{+}, \tag{2.13}$$

☞ 362

PSEUDO-INVERSE

☞ 358

where the $p \times n$ matrix $\mathbf{X}^{+}$ in (2.13) is the *pseudo-inverse* of $\mathbf{X}$. If $\mathbf{X}$ happens to be of *full column rank* (so that none of the columns can be expressed as a linear combination of the other columns), then $\mathbf{X}^{+} = (\mathbf{X}^{\top}\mathbf{X})^{-1}\mathbf{X}^{\top}$.

In any case, from $\mathbf{X}\widehat{\boldsymbol{\beta}} = \mathbf{P}\boldsymbol{y}$ and $\mathbf{P}\mathbf{X} = \mathbf{X}$, we can see that $\widehat{\boldsymbol{\beta}}$ satisfies the *normal equations*:

NORMAL EQUATIONS

$$\mathbf{X}^{\top}\mathbf{X}\boldsymbol{\beta} = \mathbf{X}^{\top}\mathbf{P}\boldsymbol{y} = (\mathbf{P}\mathbf{X})^{\top}\boldsymbol{y} = \mathbf{X}^{\top}\boldsymbol{y}. \tag{2.14}$$

This is a set of linear equations, which can be solved very fast and whose solution can be written explicitly as:

$$\widehat{\boldsymbol{\beta}} = \mathbf{X}^{+}\boldsymbol{y}. \tag{2.15}$$

Figure 2.6 shows the trained learners for various values of p:

$$h_{\tau}^{\mathcal{H}_p}(u) = g_{\tau}^{\mathcal{G}_p}(\boldsymbol{x}) = \boldsymbol{x}^{\top}\widehat{\boldsymbol{\beta}}$$

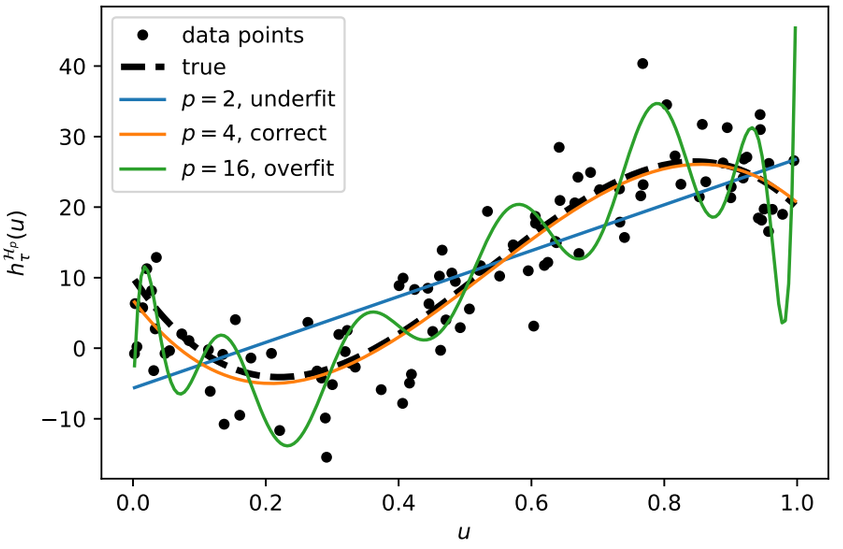


Figure 2.6: Training data with fitted curves for $p = 2, 4$, and 16. The true cubic polynomial curve for $p = 4$ is also plotted (dashed line).

We see that for $p = 16$ the fitted curve lies closer to the data points, but is further away from the dashed true polynomial curve, indicating that we overfit. The choice $p = 4$ (the true cubic polynomial) is much better than $p = 16$, or indeed $p = 2$ (straight line).

Each function class $\mathcal{G}_p$ gives a different learner $g_\tau^{\mathcal{G}_p}$, $p = 1, 2, \ldots$. To assess which is better, we should not simply take the one that gives the smallest training loss. We can always get a *zero* training loss by taking $p = n$, because for any set of n points there exists a polynomial of degree $n - 1$ that interpolates all points!

Instead, we assess the predictive performance of the learners using the test loss (2.7), computed from a test data set. If we collect all n' test feature vectors in a matrix $\mathbf{X}'$ and the corresponding test responses in a vector $\boldsymbol{y}'$, then, similar to (2.11), the test loss can be written compactly as

$$\ell_{\tau'}(g_\tau^{\mathcal{G}_p}) = \frac{1}{n'} \|\boldsymbol{y}' - \mathbf{X}'\widehat{\boldsymbol{\beta}}\|^2,$$

where $\widehat{\boldsymbol{\beta}}$ is given by (2.15), using the training data.

Figure 2.7 shows a plot of the test loss against the number of parameters in the vector $\boldsymbol{\beta}$; that is, p. The graph has a characteristic "bath-tub" shape and is at its lowest for $p = 4$, correctly identifying the polynomial order 3 for the true model. Note that the test loss, as an estimate for the generalization risk (2.7), becomes numerically unreliable after $p = 16$ (the graph goes down, where it should go up). The reader may check that the graph for the training loss exhibits a similar numerical instability for large p, and in fact fails to numerically decrease to 0 for large p, contrary to what it should do in theory. The numerical problems arise from the fact that for large p the columns of the (Vandermonde) matrix $\mathbf{X}$ are of vastly different magnitudes and so floating point errors quickly become very large.

Finally, observe that the lower bound for the test loss is here around 21, which corresponds to an estimate of the minimal (squared-error) risk $\ell^* = 25$.

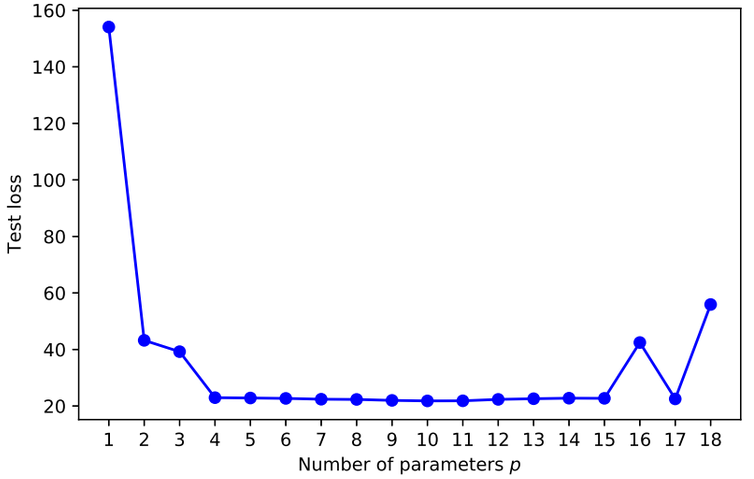


Figure 2.7: Test loss as function of the number of parameters p of the model.

This script shows how the training data were generated and plotted in Python:

polyreg1.py

```
import numpy as np
from numpy.random import rand , randn
from numpy.linalg import norm , solve
import matplotlib.pyplot as plt
def generate_data(beta , sig, n):
   u = np.random.rand(n, 1)
   y = (u ** np.arange(0, 4)) @ beta + sig * np.random.randn(n, 1)
   return u, y

np.random.seed(12)
beta = np.array([[10, -140, 400, -250]]).T
n = 100
sig = 5
u, y = generate_data(beta , sig, n)
xx = np.arange(np.min(u), np.max(u)+5e-3, 5e-3)
yy = np.polyval(np.flip(beta), xx)
plt.plot(u, y, '.', markersize=8)
plt.plot(xx, yy, '--',linewidth=3)
plt.xlabel(r'$u$')
plt.ylabel(r'$h^*(u)$')
plt.legend(['data points','true'])
plt.show()
```

The following code, which imports the code above, fits polynomial models with $p = 1, \ldots, K = 18$ parameters to the training data and plots a selection of fitted curves, as shown in Figure 2.6.

polyreg2.py

```
from polyreg1 import *

max_p = 18
p_range = np.arange(1, max_p + 1, 1)
X = np.ones((n, 1))
betahat, trainloss = {}, {}

for p in p_range:  # p is the number of parameters
    if p > 1:
        X = np.hstack((X, u**(p-1)))  # add column to matrix

    betahat[p] = solve(X.T @ X, X.T @ y)
    trainloss[p] = (norm(y - X @ betahat[p])**2/n)

p = [2, 4, 16]  # select three curves

#replot the points and true line and store in the list "plots"
plots = [plt.plot(u, y, 'k.', markersize=8)[0],
         plt.plot(xx, yy, 'k--',linewidth=3)[0]]
# add the three curves
for i in p:
    yy = np.polyval(np.flip(betahat[i]), xx)
    plots.append(plt.plot(xx, yy)[0])
```

```
plt.xlabel(r'$u$')
plt.ylabel(r'$h^{\mathcal{H}_p}_{\tau}(u)$')
plt.legend(plots,('data points', 'true','$p=2$, underfit',
                  '$p=4$, correct','$p=16$, overfit'))
plt.savefig('polyfitpy.pdf',format='pdf')
plt.show()
```

The last code snippet which imports the previous code, generates the test data and plots the graph of the test loss, as shown in Figure 2.7.

polyreg3.py

```
from polyreg2 import *

# generate test data
u_test, y_test = generate_data(beta, sig, n)

MSE = []
X_test = np.ones((n, 1))

for p in p_range:
    if p > 1:
        X_test = np.hstack((X_test, u_test**(p-1)))

    y_hat = X_test @ betahat[p]  # predictions
    MSE.append(np.sum((y_test - y_hat)**2/n))

plt.plot(p_range, MSE, 'b', p_range, MSE, 'bo')
plt.xticks(ticks=p_range)
plt.xlabel('Number of parameters $p$')
plt.ylabel('Test loss')
```

2.4 Tradeoffs in Statistical Learning

The art of machine learning in the supervised case is to make the generalization risk (2.5) or expected generalization risk (2.6) as small as possible, while using as few computational resources as possible. In pursuing this goal, a suitable class $\mathcal{G}$ of prediction functions has to be chosen. This choice is driven by various factors, such as

- the complexity of the class (e.g., is it rich enough to adequately approximate, or even contain, the optimal prediction function g^*?),
- the ease of training the learner via the optimization program (2.4),
- how accurately the training loss (2.3) estimates the risk (2.1) within class $\mathcal{G}$,
- the feature types (categorical, continuous, etc.).

As a result, the choice of a suitable function class $\mathcal{G}$ usually involves a tradeoff between conflicting factors. For example, a learner from a simple class $\mathcal{G}$ can be trained very

quickly, but may not approximate g^* very well, whereas a learner from a rich class $\mathcal{G}$ that contains g^* may require a lot of computing resources to train.

To better understand the relation between model complexity, computational simplicity, and estimation accuracy, it is useful to decompose the generalization risk into several parts, so that the tradeoffs between these parts can be studied. We will consider two such decompositions: the approximation–estimation tradeoff and the bias–variance tradeoff.

We can decompose the generalization risk (2.5) into the following three components:

$$\ell(g_\tau^{\mathcal{G}}) = \underbrace{\ell^*}_{\text{irreducible risk}} + \underbrace{\ell(g^{\mathcal{G}}) - \ell^*}_{\text{approximation error}} + \underbrace{\ell(g_\tau^{\mathcal{G}}) - \ell(g^{\mathcal{G}})}_{\text{statistical error}}, \tag{2.16}$$

IRREDUCIBLE RISK

where $\ell^* := \ell(g^*)$ is the *irreducible risk* and $g^{\mathcal{G}} := \operatorname{argmin}_{g \in \mathcal{G}} \ell(g)$ is the best learner within class $\mathcal{G}$. No learner can predict a new response with a smaller risk than ℓ^*.

APPROXIMATION ERROR

The second component is the *approximation error*; it measures the difference between the irreducible risk and the best possible risk that can be obtained by selecting the best prediction function in the selected class of functions $\mathcal{G}$. Determining a suitable class $\mathcal{G}$ and minimizing $\ell(g)$ over this class is purely a problem of numerical and functional analysis, as the training data τ are not present. For a fixed $\mathcal{G}$ that does not contain the optimal g^*, the approximation error cannot be made arbitrarily small and may be the dominant component in the generalization risk. The only way to reduce the approximation error is by expanding the class $\mathcal{G}$ to include a larger set of possible functions.

STATISTICAL (ESTIMATION) ERROR

The third component is the *statistical (estimation) error*. It depends on the training set τ and, in particular, on how well the learner $g_\tau^{\mathcal{G}}$ estimates the best possible prediction function, $g^{\mathcal{G}}$, within class $\mathcal{G}$. For any sensible estimator this error should decay to zero (in probability or expectation) as the training size tends to infinity.

☞ 441

APPROXIMATION–ESTIMATION TRADEOFF

The *approximation–estimation tradeoff* pits two competing demands against each other. The first is that the class $\mathcal{G}$ has to be simple enough so that the statistical error is not too large. The second is that the class $\mathcal{G}$ has to be rich enough to ensure a small approximation error. Thus, there is a tradeoff between the approximation and estimation errors.

For the special case of the squared-error loss, the generalization risk is equal to $\ell(g_\tau^{\mathcal{G}}) = \mathbb{E}(Y - g_\tau^{\mathcal{G}}(\boldsymbol{X}))^2$; that is, the expected squared error[1] between the predicted value $g_\tau^{\mathcal{G}}(\boldsymbol{X})$ and the response Y. Recall that in this case the optimal prediction function is given by $g^*(\boldsymbol{x}) = \mathbb{E}[Y \,|\, \boldsymbol{X} = \boldsymbol{x}]$. The decomposition (2.16) can now be interpreted as follows.

1. The first component, $\ell^* = \mathbb{E}(Y - g^*(\boldsymbol{X}))^2$, is the *irreducible error*, as no prediction function will yield a smaller expected squared error.

2. The second component, the approximation error $\ell(g^{\mathcal{G}}) - \ell(g^*)$, is equal to $\mathbb{E}(g^{\mathcal{G}}(\boldsymbol{X}) - g^*(\boldsymbol{X}))^2$. We leave the proof (which is similar to that of Theorem 2.1) as an exercise; see Exercise 2. Thus, the approximation error (defined as a risk difference) can here be interpreted as the expected squared error between the optimal predicted value and the optimal predicted value within the class $\mathcal{G}$.

3. For the third component, the statistical error, $\ell(g_\tau^{\mathcal{G}}) - \ell(g^{\mathcal{G}})$ there is no direct interpretation as an expected squared error *unless* $\mathcal{G}$ is the class of *linear* functions; that is, $g(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta}$ for some vector $\boldsymbol{\beta}$. In this case we can write (see Exercise 3) the statistical error as $\ell(g_\tau^{\mathcal{G}}) - \ell(g^{\mathcal{G}}) = \mathbb{E}(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - g^{\mathcal{G}}(\boldsymbol{X}))^2$.

[1] Colloquially called *mean squared error*.

Thus, when using a squared-error loss, the generalization risk for a linear class $\mathcal{G}$ can be decomposed as:

$$\ell(g_\tau^{\mathcal{G}}) = \mathbb{E}(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - Y)^2 = \ell^* + \underbrace{\mathbb{E}(g^{\mathcal{G}}(\boldsymbol{X}) - g^*(\boldsymbol{X}))^2}_{\text{approximation error}} + \underbrace{\mathbb{E}(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - g^{\mathcal{G}}(\boldsymbol{X}))^2}_{\text{statistical error}}. \tag{2.17}$$

Note that in this decomposition the statistical error is the only term that depends on the training set.

■ **Example 2.2 (Polynomial Regression (cont.))** We continue Example 2.1. Here $\mathcal{G} = \mathcal{G}_p$ is the class of linear functions of $\boldsymbol{x} = [1, u, u^2, \ldots, u^{p-1}]^\top$, and $g^*(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta}^*$. Conditional on $\boldsymbol{X} = \boldsymbol{x}$ we have that $Y = g^*(\boldsymbol{x}) + \varepsilon(\boldsymbol{x})$, with $\varepsilon(\boldsymbol{x}) \sim \mathcal{N}(0, \ell^*)$, where $\ell^* = \mathbb{E}(Y - g^*(\boldsymbol{X}))^2 = 25$ is the irreducible error. We wish to understand how the approximation and statistical errors behave as we change the complexity parameter p.

First, we consider the approximation error. Any function $g \in \mathcal{G}_p$ can be written as

$$g(\boldsymbol{x}) = h(u) = \beta_1 + \beta_2 u + \cdots + \beta_p u^{p-1} = [1, u, \ldots, u^{p-1}]\boldsymbol{\beta},$$

and so $g(\boldsymbol{X})$ is distributed as $[1, U, \ldots, U^{p-1}]\boldsymbol{\beta}$, where $U \sim \mathcal{U}(0, 1)$. Similarly, $g^*(\boldsymbol{X})$ is distributed as $[1, U, U^2, U^3]\boldsymbol{\beta}^*$. It follows that an expression for the approximation error is: $\int_0^1 \left([1, u, \ldots, u^{p-1}]\boldsymbol{\beta} - [1, u, u^2, u^3]\boldsymbol{\beta}^*\right)^2 \mathrm{d}u$. To minimize this error, we set the gradient with respect to $\boldsymbol{\beta}$ to zero and obtain the p linear equations ☞ 399

$$\begin{aligned}
\int_0^1 \left([1, u, \ldots, u^{p-1}]\boldsymbol{\beta} - [1, u, u^2, u^3]\boldsymbol{\beta}^*\right) \mathrm{d}u &= 0,\\
\int_0^1 \left([1, u, \ldots, u^{p-1}]\boldsymbol{\beta} - [1, u, u^2, u^3]\boldsymbol{\beta}^*\right) u\,\mathrm{d}u &= 0,\\
&\vdots\\
\int_0^1 \left([1, u, \ldots, u^{p-1}]\boldsymbol{\beta} - [1, u, u^2, u^3]\boldsymbol{\beta}^*\right) u^{p-1}\mathrm{d}u &= 0.
\end{aligned}$$

Let

$$\mathbf{H}_p = \int_0^1 [1, u, \ldots, u^{p-1}]^\top [1, u, \ldots, u^{p-1}]\,\mathrm{d}u$$

be the $p \times p$ *Hilbert matrix*, which has (i, j)-th entry given by $\int_0^1 u^{i+j-2}\,\mathrm{d}u = 1/(i + j - 1)$. Then, the above system of linear equations can be written as $\mathbf{H}_p\boldsymbol{\beta} = \widetilde{\mathbf{H}}\boldsymbol{\beta}^*$, where $\widetilde{\mathbf{H}}$ is the $p \times 4$ upper left sub-block of $\mathbf{H}_{\widetilde{p}}$ and $\widetilde{p} = \max\{p, 4\}$. The solution, which we denote by $\boldsymbol{\beta}_p$, is: HILBERT MATRIX

$$\boldsymbol{\beta}_p = \begin{cases} \frac{65}{6}, & p = 1,\\ [-\frac{20}{3}, 35]^\top, & p = 2,\\ [-\frac{5}{2}, 10, 25]^\top, & p = 3,\\ [10, -140, 400, -250, 0, \ldots, 0]^\top, & p \geqslant 4. \end{cases} \tag{2.18}$$

Hence, the approximation error $\mathbb{E}\left(g^{\mathcal{G}_p}(\boldsymbol{X}) - g^*(\boldsymbol{X})\right)^2$ is given by

$$\int_0^1 \left([1, u, \ldots, u^{p-1}]\boldsymbol{\beta}_p - [1, u, u^2, u^3]\boldsymbol{\beta}^*\right)^2 \mathrm{d}u = \begin{cases} \frac{32225}{252} \approx 127.9, & p = 1,\\ \frac{1625}{63} \approx 25.8, & p = 2,\\ \frac{625}{28} \approx 22.3, & p = 3,\\ 0, & p \geqslant 4. \end{cases} \tag{2.19}$$

Notice how the approximation error becomes smaller as p increases. In this particular example the approximation error is in fact zero for $p \geqslant 4$. In general, as the class of approximating functions $\mathcal{G}$ becomes more complex, the approximation error goes down.

Next, we illustrate the typical behavior of the statistical error. Since $g_\tau(\boldsymbol{x}) = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}$, the statistical error can be written as

$$\int_0^1 \left([1, \ldots, u^{p-1}](\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p)\right)^2 \mathrm{d}u = (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p)^\top \mathbf{H}_p (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p). \tag{2.20}$$

Figure 2.8 illustrates the decomposition (2.17) of the generalization risk for the *same* training set that was used to compute the test loss in Figure 2.7. Recall that test loss gives an estimate of the generalization risk, using independent test data. Comparing the two figures, we see that in this case the two match closely. The global minimum of the statistical error is approximately 0.28, with minimizer $p = 4$. Since the approximation error is monotonically decreasing to zero, $p = 4$ is also the global minimizer of the generalization risk.

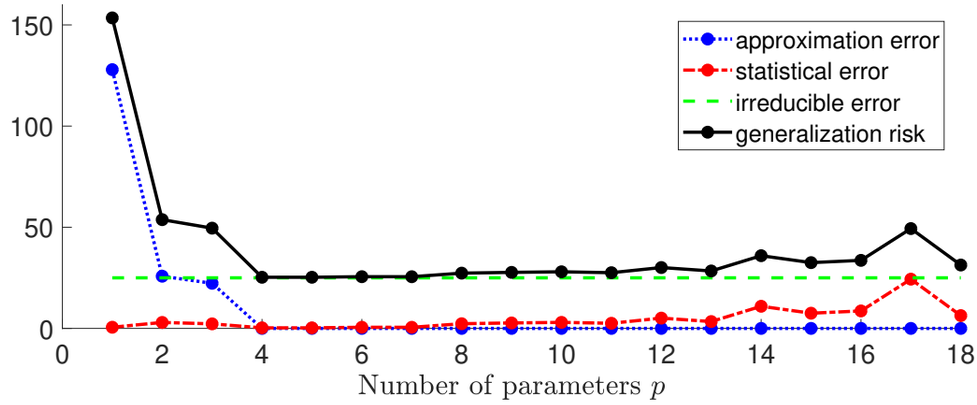


Figure 2.8: The generalization risk for a particular training set is the sum of the irreducible error, the approximation error, and the statistical error. The approximation error decreases to zero as p increases, whereas the statistical error has a tendency to increase after $p = 4$.

Note that the statistical error depends on the estimate $\widehat{\boldsymbol{\beta}}$, which in its turn depends on the training set τ. We can obtain a better understanding of the statistical error by considering its *expected* behavior; that is, averaged over many training sets. This is explored in Exercise 11. ■

Using again a squared-error loss, a second decomposition (for general $\mathcal{G}$) starts from

$$\ell(g_\tau^{\mathcal{G}}) = \ell^* + \ell(g_\tau^{\mathcal{G}}) - \ell(g^*),$$

where the statistical error and approximation error are combined. Using similar reasoning as in the proof of Theorem 2.1, we have

$$\ell(g_\tau^{\mathcal{G}}) = \mathbb{E}(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - Y)^2 = \ell^* + \mathbb{E}\left(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - g^*(\boldsymbol{X})\right)^2 = \ell^* + \mathbb{E}D^2(\boldsymbol{X}, \tau),$$

where $D(\boldsymbol{x}, \tau) := g_\tau^{\mathcal{G}}(\boldsymbol{x}) - g^*(\boldsymbol{x})$. Now consider the random variable $D(\boldsymbol{x}, \mathcal{T})$ for a random training set $\mathcal{T}$. The expectation of its square is:

$$\begin{aligned}\mathbb{E}\left(g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x}) - g^*(\boldsymbol{x})\right)^2 &= \mathbb{E}D^2(\boldsymbol{x}, \mathcal{T}) = (\mathbb{E}D(\boldsymbol{x}, \mathcal{T}))^2 + \mathbb{V}\mathrm{ar}\, D(\boldsymbol{x}, \mathcal{T}) \\ &= \underbrace{(\mathbb{E}g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x}) - g^*(\boldsymbol{x}))^2}_{\text{pointwise squared bias}} + \underbrace{\mathbb{V}\mathrm{ar}\, g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x})}_{\text{pointwise variance}} . \end{aligned} \tag{2.21}$$

If we view the learner $g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x})$ as a function of a random training set, then the *pointwise squared bias* term is a measure for how close $g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x})$ is on average to the true $g^*(\boldsymbol{x})$, whereas the *pointwise variance* term measures the deviation of $g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x})$ from its expected value $\mathbb{E}g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{x})$. The squared bias can be reduced by making the class of functions $\mathcal{G}$ more complex. However, decreasing the bias by increasing the complexity often leads to an increase in the variance term. We are thus seeking learners that provide an optimal balance between the bias and variance, as expressed via a minimal generalization risk. This is called the *bias–variance tradeoff*.

POINTWISE SQUARED BIAS
POINTWISE VARIANCE
BIAS–VARIANCE TRADEOFF

Note that the *expected* generalization risk (2.6) can be written as $\ell^* + \mathbb{E}D^2(\boldsymbol{X}, \mathcal{T})$, where $\boldsymbol{X}$ and $\mathcal{T}$ are independent. It therefore decomposes as

$$\mathbb{E}\,\ell(g_{\mathcal{T}}^{\mathcal{G}}) = \ell^* + \underbrace{\mathbb{E}\,(\mathbb{E}[g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{X}) \,|\, \boldsymbol{X}] - g^*(\boldsymbol{X}))^2}_{\text{expected squared bias}} + \underbrace{\mathbb{E}[\mathbb{V}\mathrm{ar}[g_{\mathcal{T}}^{\mathcal{G}}(\boldsymbol{X}) \,|\, \boldsymbol{X}]]}_{\text{expected variance}} . \tag{2.22}$$

2.5 Estimating Risk

The most straightforward way to quantify the generalization risk (2.5) is to estimate it via the test loss (2.7). However, the generalization risk depends inherently on the training set, and so different training sets may yield significantly different estimates. Moreover, when there is a limited amount of data available, reserving a substantial proportion of the data for testing rather than training may be uneconomical. In this section we consider different methods for estimating risk measures which aim to circumvent these difficulties.

2.5.1 In-Sample Risk

We mentioned that, due to the phenomenon of overfitting, the training loss of the learner, $\ell_\tau(g_\tau)$ (for simplicity, here we omit $\mathcal{G}$ from $g_\tau^{\mathcal{G}}$), is not a good estimate of the generalization risk $\ell(g_\tau)$ of the learner. One reason for this is that we use the same data for both training the model and assessing its risk. How should we then estimate the generalization risk or expected generalization risk?

To simplify the analysis, suppose that we wish to estimate the average accuracy of the predictions of the learner g_τ at the n feature vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ (these are part of the training set τ). In other words, we wish to estimate the *in-sample risk* of the learner g_τ:

IN-SAMPLE RISK

$$\ell_{\text{in}}(g_\tau) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\,\mathrm{Loss}(Y_i', g_\tau(\boldsymbol{x}_i)), \tag{2.23}$$

where each response Y_i' is drawn from $f(y \,|\, \boldsymbol{x}_i)$, independently. Even in this simplified setting, the training loss of the learner will be a poor estimate of the in-sample risk. Instead, the

proper way to assess the prediction accuracy of the learner at the feature vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, is to draw new response values $Y_i' \sim f(y \,|\, \boldsymbol{x}_i)$, $i = 1, \ldots, n$, that are independent from the responses $y_1, \ldots, y_n$ in the training data, and then estimate the in-sample risk of g_τ via

$$\frac{1}{n} \sum_{i=1}^{n} \text{Loss}(Y_i', g_\tau(\boldsymbol{x}_i)).$$

For a fixed training set τ, we can compare the training loss of the learner with the in-sample risk. Their difference,

$$\text{op}_\tau = \ell_{\text{in}}(g_\tau) - \ell_\tau(g_\tau),$$

is called the *optimism* (of the training loss), because it measures how much the training loss underestimates (is optimistic about) the unknown in-sample risk. Mathematically, it is simpler to work with the *expected optimism*:

EXPECTED OPTIMISM

$$\mathbb{E}[\text{op}_\mathcal{T} \,|\, \boldsymbol{X}_1 = \boldsymbol{x}_1, \ldots, \boldsymbol{X}_n = \boldsymbol{x}_n] =: \mathbb{E}_\mathbf{X} \, \text{op}_\mathcal{T},$$

where the expectation is taken over a random training set $\mathcal{T}$, conditional on $\boldsymbol{X}_i = \boldsymbol{x}_i$, $i = 1, \ldots, n$. For ease of notation, we have abbreviated the expected optimism to $\mathbb{E}_\mathbf{X} \, \text{op}_\mathcal{T}$, where $\mathbb{E}_\mathbf{X}$ denotes the expectation operator conditional on $\boldsymbol{X}_i = \boldsymbol{x}_i, i = 1, \ldots, n$. As in Example 2.1, the feature vectors are stored as the rows of an $n \times p$ matrix $\mathbf{X}$. It turns out that the expected optimism for various loss functions can be expressed in terms of the (conditional) covariance between the observed and predicted response.

Theorem 2.2: Expected Optimism

For the squared-error loss and 0–1 loss with 0–1 response, the expected optimism is

$$\mathbb{E}_\mathbf{X} \, \text{op}_\mathcal{T} = \frac{2}{n} \sum_{i=1}^{n} \mathbb{C}\text{ov}_\mathbf{X}(g_\mathcal{T}(\boldsymbol{x}_i), Y_i). \tag{2.24}$$

Proof: In what follows, all expectations are taken conditional on $\boldsymbol{X}_1 = \boldsymbol{x}_1, \ldots, \boldsymbol{X}_n = \boldsymbol{x}_n$. Let Y_i be the response for $\boldsymbol{x}_i$ and let $\widehat{Y}_i = g_\mathcal{T}(\boldsymbol{x}_i)$ be the predicted value. Note that the latter depends on $Y_1, \ldots, Y_n$. Also, let Y_i' be an independent copy of Y_i for the *same* $\boldsymbol{x}_i$, as in (2.23). In particular, Y_i' has the same distribution as Y_i and is statistically independent of all $\{Y_j\}$, including Y_i, and therefore is also independent of $\widehat{Y}_i$. We have

$$\begin{aligned}
\mathbb{E}_\mathbf{X} \, \text{op}_\mathcal{T} &= \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}_\mathbf{X} \left[(Y_i' - \widehat{Y}_i)^2 - (Y_i - \widehat{Y}_i)^2 \right] = \frac{2}{n} \sum_{i=1}^{n} \mathbb{E}_\mathbf{X} \left[(Y_i - Y_i') \widehat{Y}_i \right] \\
&= \frac{2}{n} \sum_{i=1}^{n} \left(\mathbb{E}_\mathbf{X}[Y_i \widehat{Y}_i] - \mathbb{E}_\mathbf{X} Y_i \, \mathbb{E}_\mathbf{X} \widehat{Y}_i \right) = \frac{2}{n} \sum_{i=1}^{n} \mathbb{C}\text{ov}_\mathbf{X}(\widehat{Y}_i, Y_i).
\end{aligned}$$

The proof for the 0–1 loss with 0–1 response is left as Exercise 4. □

In summary, the expected optimism indicates how much, on average, the training loss deviates from the expected in-sample risk. Since the covariance of independent random variables is zero, the expected optimism is zero if the learner $g_\mathcal{T}$ is statistically independent from the responses $Y_1, \ldots, Y_n$.

■ **Example 2.3 (Polynomial Regression (cont.))** We continue Example 2.2, where the components of the response vector $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$ are independent and normally distributed with variance $\ell^* = 25$ (the irreducible error) and expectations $\mathbb{E}_{\mathbf{X}} Y_i = g^*(\boldsymbol{x}_i) = \boldsymbol{x}_i^\top \boldsymbol{\beta}^*$, $i = 1, \ldots, n$. Using the formula (2.15) for the least-squares estimator $\widehat{\boldsymbol{\beta}}$, the expected optimism (2.24) is

$$\frac{2}{n}\sum_{i=1}^{n} \mathbb{C}\mathrm{ov}_{\mathbf{X}}\left(\boldsymbol{x}_i^\top \widehat{\boldsymbol{\beta}}, Y_i\right) = \frac{2}{n}\mathrm{tr}\left(\mathbb{C}\mathrm{ov}_{\mathbf{X}}\left(\mathbf{X}\widehat{\boldsymbol{\beta}}, \boldsymbol{Y}\right)\right) = \frac{2}{n}\mathrm{tr}\left(\mathbb{C}\mathrm{ov}_{\mathbf{X}}\left(\mathbf{X}\mathbf{X}^+\boldsymbol{Y}, \boldsymbol{Y}\right)\right)$$
$$= \frac{2\mathrm{tr}\left(\mathbf{X}\mathbf{X}^+\mathbb{C}\mathrm{ov}_{\mathbf{X}}\left(\boldsymbol{Y}, \boldsymbol{Y}\right)\right)}{n} = \frac{2\ell^*\mathrm{tr}\left(\mathbf{X}\mathbf{X}^+\right)}{n} = \frac{2\ell^* p}{n}.$$

In the last equation we used the cyclic property of the trace (Theorem A.1): $\mathrm{tr}(\mathbf{X}\mathbf{X}^+) = \mathrm{tr}(\mathbf{X}^+\mathbf{X}) = \mathrm{tr}(\mathbf{I}_p)$, assuming that $\mathrm{rank}(\mathbf{X}) = p$. Therefore, an estimate for the in-sample risk (2.23) is: ☞ 359

$$\widehat{\ell}_{\mathrm{in}}(g_\tau) = \ell_\tau(g_\tau) + 2\ell^* p/n, \tag{2.25}$$

where we have assumed that the irreducible risk ℓ^* is known. Figure 2.9 shows that this estimate is very close to the test loss from Figure 2.7. Hence, instead of computing the test loss to assess the best model complexity p, we could simply have minimized the training loss plus the correction term $2\ell^* p/n$. In practice, ℓ^* also has to be estimated somehow.

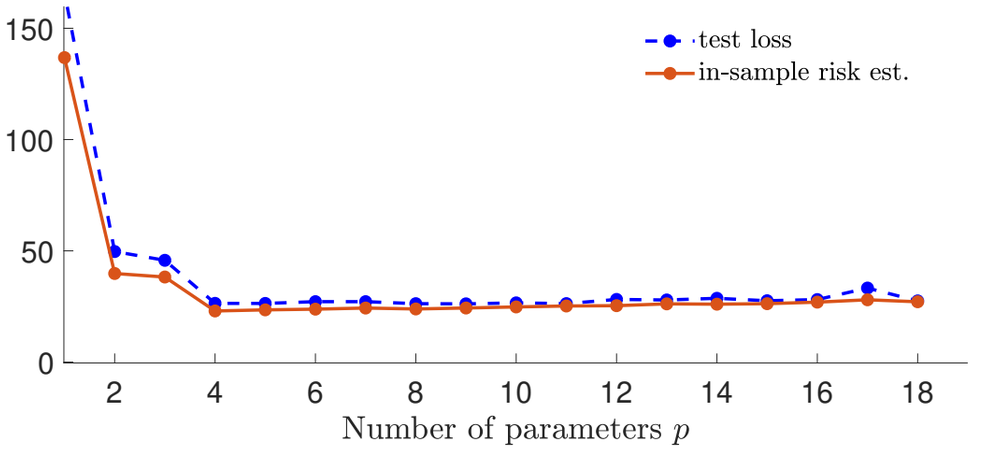


Figure 2.9: In-sample risk estimate $\widehat{\ell}_{\mathrm{in}}(g_\tau)$ as a function of the number of parameters p of the model. The test loss is superimposed as a blue dashed curve.

■

2.5.2 Cross-Validation

In general, for complex function classes $\mathcal{G}$, it is very difficult to derive simple formulas of the approximation and statistical errors, let alone for the generalization risk or expected generalization risk. As we saw, when there is an abundance of data, the easiest way to assess the generalization risk for a given training set τ is to obtain a test set τ' and evaluate the test loss (2.7). When a sufficiently large test set is not available but computational resources are cheap, one can instead gain direct knowledge of the expected generalization risk via a computationally intensive method called *cross-validation*. ☞ 24

CROSS-VALIDATION

The idea is to make multiple identical copies of the data set, and to partition each copy into different training and test sets, as illustrated in Figure 2.10. Here, there are four copies of the data set (consisting of response and explanatory variables). Each copy is divided into a test set (colored blue) and training set (colored pink). For each of these sets, we estimate the model parameters using only training data and then predict the responses for the test set. The average loss between the predicted and observed responses is then a measure for the predictive power of the model.

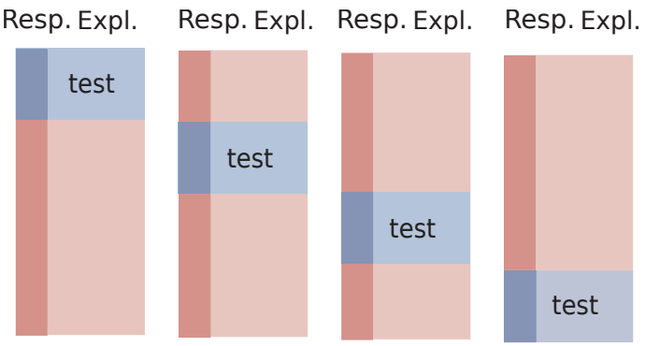


Figure 2.10: An illustration of four-fold cross-validation, representing four copies of the same data set. The data in each copy is partitioned into a training set (pink) and a test set (blue). The darker columns represent the response variable and the lighter ones the explanatory variables.

FOLDS

In particular, suppose we partition a data set $\mathcal{T}$ of size n into K *folds* $C_1, \ldots, C_K$ of sizes $n_1, \ldots, n_K$ (hence, $n_1 + \cdots + n_K = n$). Typically $n_k \approx n/K$, $k = 1, \ldots, K$.

Let ℓ_{C_k} be the test loss when using C_k as test data and all remaining data, denoted $\mathcal{T}_{-k}$, as training data. Each ℓ_{C_k} is an unbiased estimator of the generalization risk for training set $\mathcal{T}_{-k}$; that is, for $\ell(g_{\mathcal{T}_{-k}})$.

K-FOLD CROSS-VALIDATION

The *K-fold cross-validation* loss is the weighted average of these risk estimators:

$$\begin{aligned} \mathrm{CV}_K &= \sum_{k=1}^{K} \frac{n_k}{n} \ell_{C_k}(g_{\mathcal{T}_{-k}}) \\ &= \frac{1}{n} \sum_{k=1}^{K} \sum_{i \in C_k} \mathrm{Loss}(g_{\mathcal{T}_{-k}}(\boldsymbol{x}_i), y_i) \\ &= \frac{1}{n} \sum_{i=1}^{n} \mathrm{Loss}(g_{\mathcal{T}_{-\kappa(i)}}(\boldsymbol{x}_i), y_i), \end{aligned}$$

where the function $\kappa : \{1, \ldots, n\} \mapsto \{1, \ldots, K\}$ indicates to which of the K folds each of the n observations belongs. As the average is taken over varying training sets $\{\mathcal{T}_{-k}\}$, it estimates the expected generalization risk $\mathbb{E}\,\ell(g_{\mathcal{T}})$, rather than the generalization risk $\ell(g_\tau)$ for the particular training set τ.

■ **Example 2.4 (Polynomial Regression (cont.))** For the polynomial regression example, we can calculate a K-fold cross-validation loss with a nonrandom partitioning of the training set using the following code, which imports the previous code for the polynomial regression example. We omit the full plotting code.

polyregCV.py

```
from polyreg3 import *

K_vals = [5, 10, 100]  # number of folds
cv = np.zeros((len(K_vals), max_p))   # cv loss
X = np.ones((n, 1))

for p in p_range:
  if p > 1:
    X = np.hstack((X, u**(p-1)))
  j = 0
  for K in K_vals:
    loss = []
    for k in range(1, K+1):
       # integer indices of test samples
       test_ind = ((n/K)*(k-1) + np.arange(1,n/K+1)-1).astype('int')
       train_ind = np.setdiff1d(np.arange(n), test_ind)

       X_train, y_train = X[train_ind, :], y[train_ind, :]
       X_test, y_test = X[test_ind, :], y[test_ind]

       # fit model and evaluate test loss
       betahat = solve(X_train.T @ X_train, X_train.T @ y_train)
       loss.append(norm(y_test - X_test @ betahat) ** 2)

    cv[j, p-1] = sum(loss)/n
    j += 1

# basic plotting
plt.plot(p_range, cv[0, :], 'k-.')
plt.plot(p_range, cv[1, :], 'r')
plt.plot(p_range, cv[2, :], 'b--')
plt.show()
```

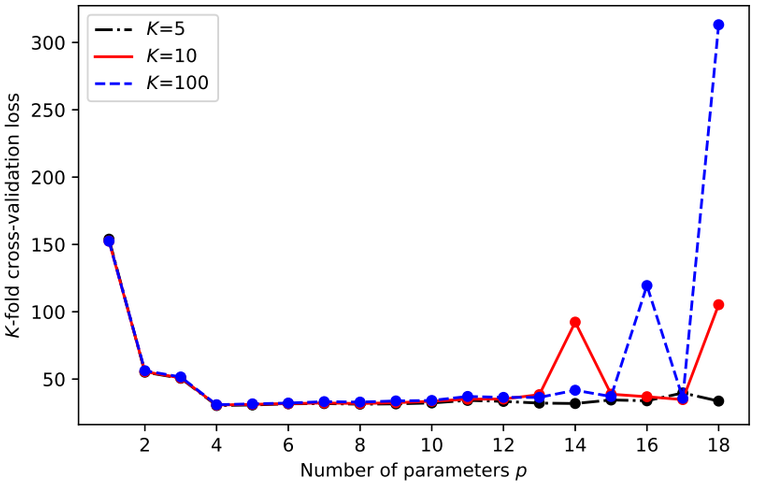


Figure 2.11: K-fold cross-validation for the polynomial regression example.

Figure 2.11 shows the cross-validation loss for $K \in \{5, 10, 100\}$. The case $K = 100$ corresponds to the *leave-one-out cross-validation*, which can be computed more efficiently using the formula in Theorem 5.1. ■

LEAVE-ONE-OUT CROSS-VALIDATION

☞ 174

2.6 Modeling Data

MODEL

The first step in any data analysis is to *model* the data in one form or another. For example, in an *unsupervised* learning setting with data represented by a vector $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$, a very general model is to assume that $\boldsymbol{x}$ is the outcome of a random vector $\boldsymbol{X} = [X_1, \ldots, X_p]^\top$ with some unknown pdf f. The model can then be refined by assuming a specific form of f.

When given a sequence of such data vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, one of the simplest models is to assume that the corresponding random vectors $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ are *independent and identically distributed (iid)*. We write

☞ 431

$$\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n \overset{\text{iid}}{\sim} f \quad \text{or} \quad \boldsymbol{X}_1, \ldots, \boldsymbol{X}_n \overset{\text{iid}}{\sim} \mathsf{Dist},$$

to indicate that the random vectors form an iid sample from a sampling pdf f or sampling distribution Dist. This model formalizes the notion that the knowledge about one variable does not provide extra information about another variable. The main theoretical use of independent data models is that the joint density of the random vectors $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ is simply the *product* of the marginal ones; see Theorem C.1. Specifically,

☞ 431

$$f_{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = f(\boldsymbol{x}_1) \cdots f(\boldsymbol{x}_n).$$

In most models of this kind, our approximation or model for the sampling distribution is specified up to a small number of parameters. That is, $g(\boldsymbol{x})$ is of the form $g(\boldsymbol{x} \,|\, \boldsymbol{\beta})$ which is known up to some parameter vector $\boldsymbol{\beta}$. Examples for the one-dimensional case ($p = 1$) include the $\mathcal{N}(\mu, \sigma^2)$, $\mathsf{Bin}(n, p)$, and $\mathsf{Exp}(\lambda)$ distributions. See Tables C.1 and C.2 for other common sampling distributions.

☞ 427

Typically, the parameters are unknown and must be estimated from the data. In a nonparametric setting the whole sampling distribution would be unknown. To visualize the underlying sampling distribution from outcomes $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ one can use graphical representations such as histograms, density plots, and empirical cumulative distribution functions, as discussed in Chapter 1.

☞ 11

If the order in which the data were collected (or their labeling) is not informative or relevant, then the joint pdf of $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ satisfies the symmetry:

$$f_{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = f_{\boldsymbol{X}_{\pi_1}, \ldots, \boldsymbol{X}_{\pi_n}}(\boldsymbol{x}_{\pi_1}, \ldots, \boldsymbol{x}_{\pi_n}) \tag{2.26}$$

for any permutation $\pi_1, \ldots, \pi_n$ of the integers $1, \ldots, n$. We say that the infinite sequence $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots$ is *exchangeable* if this permutational invariance (2.26) holds for any finite subset of the sequence. As we shall see in Section 2.9 on Bayesian learning, it is common to assume that the random vectors $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ are a subset of an exchangeable sequence and thus satisfy (2.26). Note that while iid random variables are exchangeable, the converse is not necessarily true. Thus, the assumption of an exchangeable sequence of random vectors is weaker than the assumption of iid random vectors.

EXCHANGEABLE

Figure 2.12 illustrates the modeling tradeoffs. The keywords within the triangle represent various modeling paradigms. A few keywords have been highlighted, symbolizing their importance in modeling. The specific meaning of the keywords does not concern us here, but the point is there are many models to choose from, depending on what assumptions are made about the data.

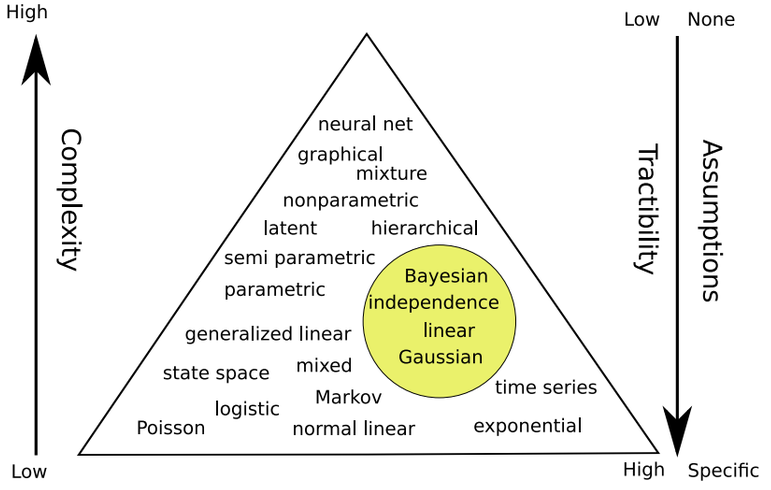


Figure 2.12: Illustration of the modeling dilemma. Complex models are more generally applicable, but may be difficult to analyze. Simple models may be highly tractable, but may not describe the data accurately. The triangular shape signifies that there are a great many specific models but not so many generic ones.

On the one hand, models that make few assumptions are more widely applicable, but at the same time may not be very mathematically tractable or provide insight into the nature of the data. On the other hand, very specific models may be easy to handle and interpret, but may not match the data very well. This tradeoff between the tractability and applicability of the model is very similar to the approximation–estimation tradeoff described in Section 2.4.

In the typical *unsupervised* setting we have a training set $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ that is viewed as the outcome of n iid random variables $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ from some unknown pdf f. The objective is then to learn or estimate f from the finite training data. To put the learning in a similar framework as for supervised learning discussed in the preceding Sections 2.3–2.5, we begin by specifying a class of probability density functions $\mathcal{G}_p := \{g(\cdot \,|\, \boldsymbol{\theta}), \boldsymbol{\theta} \in \boldsymbol{\Theta}\}$, where $\boldsymbol{\theta}$ is a parameter in some subset $\boldsymbol{\Theta}$ of $\mathbb{R}^p$. We now seek the best g in $\mathcal{G}_p$ to minimize some risk. Note that $\mathcal{G}_p$ may not necessarily contain the true f even for very large p.

We stress that our notation $g(\boldsymbol{x})$ has a different meaning in the supervised and unsupervised case. In the supervised case, g is interpreted as a prediction function for a response y; in the unsupervised setting, g is an approximation of a density f.

For each $\boldsymbol{x}$ we measure the discrepancy between the true model $f(\boldsymbol{x})$ and the hypothesized model $g(\boldsymbol{x} \,|\, \boldsymbol{\theta})$ using the loss function

$$\text{Loss}(f(\boldsymbol{x}), g(\boldsymbol{x} \,|\, \boldsymbol{\theta})) = \ln \frac{f(\boldsymbol{x})}{g(\boldsymbol{x} \,|\, \boldsymbol{\theta})} = \ln f(\boldsymbol{x}) - \ln g(\boldsymbol{x} \,|\, \boldsymbol{\theta}).$$

The expected value of this loss (that is, the risk) is thus

$$\ell(g) = \mathbb{E} \ln \frac{f(\boldsymbol{X})}{g(\boldsymbol{X} \,|\, \boldsymbol{\theta})} = \int f(\boldsymbol{x}) \ln \frac{f(\boldsymbol{x})}{g(\boldsymbol{x} \,|\, \boldsymbol{\theta})} \, \mathrm{d}\boldsymbol{x}. \tag{2.27}$$

KULLBACK–LEIBLER DIVERGENCE

The integral in (2.27) provides a fundamental way to measure the distance between two densities and is called the *Kullback–Leibler (KL) divergence*[2] between f and $g(\cdot \,|\, \boldsymbol{\theta})$. Note that the KL divergence is not symmetric in f and $g(\cdot \,|\, \boldsymbol{\theta})$. Moreover, it is always greater than or equal to 0 (see Exercise 15) and equal to 0 when $f = g(\cdot \,|\, \boldsymbol{\theta})$.

Using similar notation as for the supervised learning setting in Table 2.1, define $g^{\mathcal{G}_p}$ as the global minimizer of the risk in the class $\mathcal{G}_p$; that is, $g^{\mathcal{G}_p} = \operatorname{argmin}_{g \in \mathcal{G}_p} \ell(g)$. If we define

$$\begin{aligned} \boldsymbol{\theta}^* &= \operatorname*{argmin}_{\boldsymbol{\theta}} \mathbb{E} \operatorname{Loss}(f(\boldsymbol{X}), g(\boldsymbol{X} \,|\, \boldsymbol{\theta})) = \operatorname*{argmin}_{\boldsymbol{\theta}} \int (\ln f(\boldsymbol{x}) - \ln g(\boldsymbol{x} \,|\, \boldsymbol{\theta})) f(\boldsymbol{x}) \, \mathrm{d}\boldsymbol{x} \\ &= \operatorname*{argmax}_{\boldsymbol{\theta}} \int f(\boldsymbol{x}) \ln g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{x} = \operatorname*{argmax}_{\boldsymbol{\theta}} \mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}), \end{aligned}$$

then $g^{\mathcal{G}_p} = g(\cdot \,|\, \boldsymbol{\theta}^*)$ and learning $g^{\mathcal{G}_p}$ is equivalent to learning (or estimating) $\boldsymbol{\theta}^*$. To learn $\boldsymbol{\theta}^*$ from a training set $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ we then minimize the training loss,

$$\frac{1}{n} \sum_{i=1}^{n} \operatorname{Loss}(f(\boldsymbol{x}_i), g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta})) = -\frac{1}{n} \sum_{i=1}^{n} \ln g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}) + \frac{1}{n} \sum_{i=1}^{n} \ln f(\boldsymbol{x}_i),$$

giving:

$$\widehat{\boldsymbol{\theta}}_n := \operatorname*{argmax}_{\boldsymbol{\theta}} \frac{1}{n} \sum_{i=1}^{n} \ln g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}). \tag{2.28}$$

As the logarithm is an increasing function, this is equivalent to

$$\widehat{\boldsymbol{\theta}}_n := \operatorname*{argmax}_{\boldsymbol{\theta}} \prod_{i=1}^{n} g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}),$$

where $\prod_{i=1}^{n} g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta})$ is the *likelihood* of the data; that is, the joint density of the $\{\boldsymbol{X}_i\}$ evaluated at the points $\{\boldsymbol{x}_i\}$. We therefore have recovered the classical *maximum likelihood estimate* of $\boldsymbol{\theta}^*$.

MAXIMUM LIKELIHOOD ESTIMATE

☞ 458

When the risk $\ell(g(\cdot \,|\, \boldsymbol{\theta}))$ is convex in $\boldsymbol{\theta}$ over a convex set $\boldsymbol{\Theta}$, we can find the maximum likelihood estimator by setting the gradient of the training loss to zero; that is, we solve

$$-\frac{1}{n} \sum_{i=1}^{n} \boldsymbol{S}(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}) = \mathbf{0},$$

where $\boldsymbol{S}(\boldsymbol{x} \,|\, \boldsymbol{\theta}) := \frac{\partial \ln g(\boldsymbol{x} \,|\, \boldsymbol{\theta})}{\partial \boldsymbol{\theta}}$ is the gradient of $\ln g(\boldsymbol{x} \,|\, \boldsymbol{\theta})$ with respect to $\boldsymbol{\theta}$ and is often called the *score*.

SCORE

■ **Example 2.5 (Exponential Model)** Suppose we have the training data $\tau_n = \{x_1, \ldots, x_n\}$, which is modeled as a realization of n positive iid random variables: $X_1, \ldots, X_n \sim_{\text{iid}} f(x)$. We select the class of approximating functions $\mathcal{G}$ to be the parametric class $\{g : g(x \,|\, \theta) =$

[2] Sometimes called cross-entropy distance.

$\theta \exp(-x\theta), x > 0, \theta > 0\}$. In other words, we look for the best $g^{\mathcal{G}}$ within the family of exponential distributions with unknown parameter $\theta > 0$. The likelihood of the data is

$$\prod_{i=1}^{n} g(x_i \,|\, \theta) = \prod_{i=1}^{n} \theta \exp(-\theta x_i) = \exp(-\theta\, n\, \overline{x}_n + n \ln \theta)$$

and the score is $S(x \,|\, \theta) = -x + \theta^{-1}$. Thus, maximizing the likelihood with respect to θ is the same as maximizing $-\theta\, n\, \overline{x}_n + n \ln \theta$ or solving $-\sum_{i=1}^{n} S(x_i \,|\, \theta)/n = \overline{x}_n - \theta^{-1} = 0$. In other words, the solution to (2.28) is the maximum likelihood estimate $\widehat{\theta}_n = 1/\overline{x}_n$. ■

In a *supervised* setting, where the data is represented by a vector $\boldsymbol{x}$ of explanatory variables and a response y, the general model is that $(\boldsymbol{x}, y)$ is an outcome of $(\boldsymbol{X}, Y) \sim f$ for some unknown f. And for a training sequence $(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)$ the default model assumption is that $(\boldsymbol{X}_1, Y_1), \ldots, (\boldsymbol{X}_n, Y_n) \sim_{\text{iid}} f$. As explained in Section 2.2, the analysis primarily involves the conditional pdf $f(y \,|\, \boldsymbol{x})$ and in particular (when using the squared-error loss) the conditional expectation $g^*(\boldsymbol{x}) = \mathbb{E}[Y \,|\, \boldsymbol{X} = \boldsymbol{x}]$. The resulting representation (2.2) allows us to then write the response at $\boldsymbol{X} = \boldsymbol{x}$ as a function of the feature $\boldsymbol{x}$ plus an error term: $Y = g^*(\boldsymbol{x}) + \varepsilon(\boldsymbol{x})$.

This leads to the simplest and most important model for supervised learning, where we choose a *linear* class $\mathcal{G}$ of prediction or guess functions and assume that it is rich enough to contain the true g^*. If we further assume that, conditional on $\boldsymbol{X} = \boldsymbol{x}$, the error term ε does not depend on $\boldsymbol{x}$, that is, $\mathbb{E}\,\varepsilon = 0$ and $\mathbb{V}\text{ar}\,\varepsilon = \sigma^2$, then we obtain the following model.

Definition 2.1: Linear Model

In a *linear model* the response Y depends on a p-dimensional explanatory variable $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$ via the linear relationship

LINEAR MODEL

$$Y = \boldsymbol{x}^\top \boldsymbol{\beta} + \varepsilon, \tag{2.29}$$

where $\mathbb{E}\,\varepsilon = 0$ and $\mathbb{V}\text{ar}\,\varepsilon = \sigma^2$.

Note that (2.29) is a model for a single pair $(\boldsymbol{x}, Y)$. The model for the training set $\{(\boldsymbol{x}_i, Y_i)\}$ is simply that each Y_i satisfies (2.29) (with $\boldsymbol{x} = \boldsymbol{x}_i$) and that the $\{Y_i\}$ are independent. Gathering all responses in the vector $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$, we can write

$$\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}, \tag{2.30}$$

where $\boldsymbol{\varepsilon} = [\varepsilon_1, \ldots, \varepsilon_n]^\top$ is a vector of iid copies of ε and $\mathbf{X}$ is the so-called *model matrix*, with rows $\boldsymbol{x}_1^\top, \ldots, \boldsymbol{x}_n^\top$. Linear models are fundamental building blocks of statistical learning algorithms. For this reason, a large part of Chapter 5 is devoted to linear regression models.

MODEL MATRIX

☞ 167

■ **Example 2.6 (Polynomial Regression (cont.))** For our running Example 2.1, we see that the data is described by a linear model of the form (2.30), with model matrix $\mathbf{X}$ given in (2.10). ■

☞ 26

Before we discuss a few other models in the following sections, we would like to emphasize a number of points about modeling.

- *Any* model for data is likely to be *wrong*. For example, real data (as opposed to computer-generated data) are often assumed to come from a normal distribution, which is never exactly true. However, an important advantage of using a normal distribution is that it has many nice mathematical properties, as we will see in Section 2.7.
- Most data models depend on a number of unknown parameters, which need to be estimated from the observed data.
- Any model for real-life data needs to be *checked* for suitability. An important criterion is that data simulated from the model should resemble the observed data, at least for a certain choice of model parameters.

Here are some guidelines for choosing a model. Think of the data as a spreadsheet or data frame, as in Chapter 1, where rows represent the data units and the columns the data features (variables, groups).

- First establish the *type* of the features (quantitative, qualitative, discrete, continuous, etc.).
- Assess whether the data can be assumed to be independent across rows or columns.
- Decide on the level of generality of the model. For example, should we use a simple model with a few unknown parameters or a more generic model that has a large number of parameters? Simple specific models are easier to fit to the data (low estimation error) than more general models, but the fit itself may not be accurate (high approximation error). The tradeoffs discussed in Section 2.4 play an important role here.
- Decide on using a classical (frequentist) or Bayesian model. Section 2.9 gives a short introduction to Bayesian learning.

☞ 47

2.7 Multivariate Normal Models

A standard model for numerical observations $x_1, \ldots, x_n$ (forming, e.g., a column in a spreadsheet or data frame) is that they are the outcomes of iid normal random variables

$$X_1, \ldots, X_n \overset{\text{iid}}{\sim} \mathcal{N}(\mu, \sigma^2).$$

It is helpful to view a normally distributed random variable as a simple transformation of a standard normal random variable. To wit, if Z has a standard normal distribution, then $X = \mu + \sigma Z$ has a $\mathcal{N}(\mu, \sigma^2)$ distribution. The generalization to n dimensions is discussed in Appendix C.7. We summarize the main points: Let $Z_1, \ldots, Z_n \overset{\text{iid}}{\sim} \mathcal{N}(0, 1)$. The pdf of $\boldsymbol{Z} = [Z_1, \ldots, Z_n]^\top$ (that is, the joint pdf of $Z_1, \ldots, Z_n$) is given by

☞ 436

$$f_{\boldsymbol{Z}}(\boldsymbol{z}) = \prod_{i=1}^{n} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{1}{2} z_i^2} = (2\pi)^{-\frac{n}{2}} \mathrm{e}^{-\frac{1}{2} \boldsymbol{z}^\top \boldsymbol{z}}, \quad \boldsymbol{z} \in \mathbb{R}^n. \tag{2.31}$$

We write $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$ and say that $\boldsymbol{Z}$ has a standard normal distribution in $\mathbb{R}^n$. Let

$$\boldsymbol{X} = \boldsymbol{\mu} + \mathbf{B}\,\boldsymbol{Z} \tag{2.32}$$

for some $m \times n$ matrix $\mathbf{B}$ and m-dimensional vector $\boldsymbol{\mu}$. Then $\boldsymbol{X}$ has expectation vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$; see (C.20) and (C.21). This leads to the following definition. ☞ 434

Definition 2.2: Multivariate Normal Distribution

An m-dimensional random vector $\boldsymbol{X}$ that can be written in the form (2.32) for some m-dimensional vector $\boldsymbol{\mu}$ and $m \times n$ matrix $\mathbf{B}$, with $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$, is said to have a *multivariate normal* or *multivariate Gaussian* distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$. We write $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$.

MULTIVARIATE NORMAL

The m-dimensional density of a multivariate normal distribution has a very similar form to the density of the one-dimensional normal distribution and is given in the next theorem. We leave the proof as an exercise; see Exercise 5. ☞ 59

Theorem 2.3: Density of a Multivariate Random Vector

Let $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, where the $m \times m$ covariance matrix $\boldsymbol{\Sigma}$ is invertible. Then $\boldsymbol{X}$ has pdf

$$f_{\boldsymbol{X}}(\boldsymbol{x}) = \frac{1}{\sqrt{(2\pi)^m\,|\boldsymbol{\Sigma}|}}\, \mathrm{e}^{-\frac{1}{2}\,(\boldsymbol{x}-\boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{x}-\boldsymbol{\mu})}, \quad \boldsymbol{x} \in \mathbb{R}^m. \tag{2.33}$$

Figure 2.13 shows the pdfs of two bivariate (that is, two-dimensional) normal distributions. In both cases the mean vector is $\boldsymbol{\mu} = [0, 0]^\top$ and the variances (the diagonal elements of $\boldsymbol{\Sigma}$) are 1. The correlation coefficients (or, equivalently here, the covariances) are respectively $\varrho = 0$ and $\varrho = 0.8$.

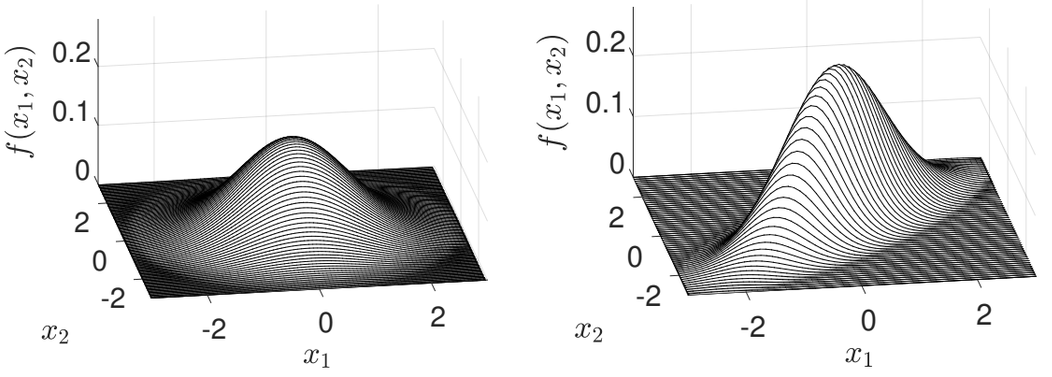


Figure 2.13: Pdfs of bivariate normal distributions with means zero, variances 1, and correlation coefficients 0 (left) and 0.8 (right).

The main reason why the multivariate normal distribution plays an important role in data science and machine learning is that it satisfies the following properties, the details and proofs of which can be found in Appendix C.7:

☞ 436

1. Affine combinations are normal.
2. Marginal distributions are normal.
3. Conditional distributions are normal.

2.8 Normal Linear Models

Normal linear models combine the simplicity of the linear model with the tractability of the Gaussian distribution. They are the principal model for traditional statistics, and include the classic linear regression and analysis of variance models.

Definition 2.3: Normal Linear Model

NORMAL LINEAR MODEL

In a *normal linear model* the response Y depends on a p-dimensional explanatory variable $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$, via the linear relationship

$$Y = \boldsymbol{x}^\top \boldsymbol{\beta} + \varepsilon, \tag{2.34}$$

where $\varepsilon \sim \mathcal{N}(0, \sigma^2)$.

Thus, a normal linear model is a linear model (in the sense of Definition 2.1) with normal error terms. Similar to (2.30), the corresponding normal linear model for the whole training set $\{(\boldsymbol{x}_i, Y_i)\}$ has the form

$$\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}, \tag{2.35}$$

where $\mathbf{X}$ is the model matrix comprised of rows $\boldsymbol{x}_1^\top, \ldots, \boldsymbol{x}_n^\top$ and $\boldsymbol{\varepsilon} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I}_n)$. Consequently, $\boldsymbol{Y}$ can be written as $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \sigma \boldsymbol{Z}$, where $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$, so that $\boldsymbol{Y} \sim \mathcal{N}(\mathbf{X}\boldsymbol{\beta}, \sigma^2 \mathbf{I}_n)$. It follows from (2.33) that its joint density is given by

☞ 45

$$g(\boldsymbol{y} \,|\, \boldsymbol{\beta}, \sigma^2, \mathbf{X}) = (2\pi\sigma^2)^{-\frac{n}{2}} \, \mathrm{e}^{-\frac{1}{2\sigma^2} \|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2}. \tag{2.36}$$

Estimation of the parameter $\boldsymbol{\beta}$ can be performed via the least-squares method, as discussed in Example 2.1. An estimate can also be obtained via the maximum likelihood method. This simply means finding the parameters σ^2 and $\boldsymbol{\beta}$ that maximize the likelihood of the outcome $\boldsymbol{y}$, given by the right-hand side of (2.36). It is clear that for every value of σ^2 the likelihood is maximal when $\|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2$ is minimal. As a consequence, the maximum likelihood estimate for $\boldsymbol{\beta}$ is the same as the least-squares estimate (2.15). We leave it as an exercise (see Exercise 18) to show that the maximum likelihood estimate of σ^2 is equal to

☞ 63

$$\widehat{\sigma^2} = \frac{\|\boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2}{n}, \tag{2.37}$$

where $\widehat{\boldsymbol{\beta}}$ is the maximum likelihood estimate (least squares estimate in this case) of $\boldsymbol{\beta}$.

2.9 Bayesian Learning

In Bayesian unsupervised learning, we seek to approximate the unknown joint density $f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ of the training data $\mathcal{T}_n = \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n\}$ via a joint pdf of the form

$$\int \left(\prod_{i=1}^{n} g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}) \right) w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}, \tag{2.38}$$

where $g(\cdot \,|\, \boldsymbol{\theta})$ belongs to a family of parametric densities $\mathcal{G}_p := \{g(\cdot \,|\, \boldsymbol{\theta}),\ \boldsymbol{\theta} \in \boldsymbol{\Theta}\}$ (viewed as a family of pdfs conditional on a parameter $\boldsymbol{\theta}$ in some set $\boldsymbol{\Theta} \subset \mathbb{R}^p$) and $w(\boldsymbol{\theta})$ is a pdf that belongs to a (possibly different) family of densities $\mathcal{W}_p$. Note how the joint pdf (2.38) satisfies the permutational invariance (2.26) and can thus be useful as a model for training data which is part of an exchangeable sequence of random variables.

Following standard practice in a Bayesian context, instead of writing $f_X(x)$ and $f_{X|Y}(x \,|\, y)$ for the pdf of X and the conditional pdf of X given Y, one simply writes $f(x)$ and $f(x \,|\, y)$. If Y is a different random variable, its pdf (at y) is thus denoted by $f(y)$.

Thus, we will use the same symbol g for different (conditional) approximating probability densities and f for the different (conditional) true and unknown probability densities. Using Bayesian notation, we can write $g(\tau \,|\, \boldsymbol{\theta}) = \prod_{i=1}^{n} g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta})$ and thus the approximating joint pdf (2.38) can then be written as $\int g(\tau \,|\, \boldsymbol{\theta}) \, w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}$ and the true unknown joint pdf as $f(\tau) = f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$.

Once $\mathcal{G}_p$ and $\mathcal{W}_p$ are specified, selecting an approximating function $g(\boldsymbol{x})$ of the form

$$g(\boldsymbol{x}) = \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) \, w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}$$

is equivalent to selecting a suitable w from $\mathcal{W}_p$. Similar to (2.27), we can use the Kullback–Leibler risk to measure the discrepancy between the proposed approximation (2.38) and the true $f(\tau)$:

$$\ell(g) = \mathbb{E} \ln \frac{f(\mathcal{T})}{\int g(\mathcal{T} \,|\, \boldsymbol{\theta}) \, w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}} = \int f(\tau) \ln \frac{f(\tau)}{\int g(\tau \,|\, \boldsymbol{\theta}) \, w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}} \, \mathrm{d}\tau. \tag{2.39}$$

The main difference with (2.27) is that since the training data is not necessarily iid (it may be exchangeable, for example), the expectation must be with respect to the joint density of $\mathcal{T}$, not with respect to the marginal $f(\boldsymbol{x})$ (as in the iid case). ☞ 40

Minimizing the training loss is equivalent to maximizing the likelihood of the training data τ; that is, solving the optimization problem

$$\max_{w \in \mathcal{W}_p} \int g(\tau \,|\, \boldsymbol{\theta}) \, w(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta},$$

where the maximization is over an appropriate class $\mathcal{W}_p$ of density functions that is believed to result in the smallest KL risk.

Suppose that we have a rough guess, denoted $w_0(\boldsymbol{\theta})$, for the best $w \in \mathcal{W}_p$ that minimizes the Kullback–Leibler risk. We can always increase the resulting likelihood $L_0 := \int g(\tau \,|\, \boldsymbol{\theta})\, w_0(\boldsymbol{\theta})\, \mathrm{d}\boldsymbol{\theta}$ by instead using the density $w_1(\boldsymbol{\theta}) := w_0(\boldsymbol{\theta})\, g(\tau \,|\, \boldsymbol{\theta})/L_0$, giving a likelihood $L_1 := \int g(\tau \,|\, \boldsymbol{\theta})\, w_1(\boldsymbol{\theta})\, \mathrm{d}\boldsymbol{\theta}$. To see this, write L_0 and L_1 as expectations with respect to w_0. In particular, we can write

$$L_0 = \mathbb{E}_{w_0}\, g(\tau \,|\, \boldsymbol{\theta}) \quad \text{and} \quad L_1 = \mathbb{E}_{w_1}\, g(\tau \,|\, \boldsymbol{\theta}) = \mathbb{E}_{w_0} g^2(\tau \,|\, \boldsymbol{\theta})/L_0.$$

It follows that

$$L_1 - L_0 = \frac{1}{L_0}\mathbb{E}_{w_0}\left[g^2(\tau \,|\, \boldsymbol{\theta}) - L_0^2\right] = \frac{1}{L_0}\mathbb{V}\mathrm{ar}_{w_0}[g(\tau \,|\, \boldsymbol{\theta})] \geqslant 0. \tag{2.40}$$

We may thus expect to obtain better predictions using w_1 instead of w_0, because w_1 has taken into account the observed data τ and increased the likelihood of the model. In fact, if we iterate this process (see Exercise 20) and create a sequence of densities $w_1, w_2, \ldots$ such that $w_t(\boldsymbol{\theta}) \propto w_{t-1}(\boldsymbol{\theta})\, g(\tau \,|\, \boldsymbol{\theta})$, then $w_t(\boldsymbol{\theta})$ concentrates more and more of its probability mass at the maximum likelihood estimator $\widehat{\boldsymbol{\theta}}$ (see (2.28)) and in the limit equals a (degenerate) point-mass pdf at $\widehat{\boldsymbol{\theta}}$. In other words, in the limit we recover the maximum likelihood method: $g_\tau(\boldsymbol{x}) = g(\boldsymbol{x} \,|\, \widehat{\boldsymbol{\theta}})$. Thus, unless the class of densities $\mathcal{W}_p$ is restricted to be non-degenerate, maximizing the likelihood as much as possible leads to a degenerate choice for $w(\boldsymbol{\theta})$.

In many situations, the maximum likelihood estimate $g(\tau \,|\, \widehat{\boldsymbol{\theta}})$ is either not an appropriate approximation to $f(\tau)$ (see Example 2.9), or simply fails to exist (see Exercise 10 in Chapter 4). In such cases, given an initial non-degenerate guess $w_0(\boldsymbol{\theta}) = g(\boldsymbol{\theta})$, one can obtain a more appropriate and non-degenerate approximation to $f(\tau)$ by taking $w(\boldsymbol{\theta}) = w_1(\boldsymbol{\theta}) \propto g(\tau \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})$ in (2.38), giving the following Bayesian learner of $f(\boldsymbol{x})$:

☞ 161

$$g_\tau(\boldsymbol{x}) := \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) \frac{g(\tau \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})}{\int g(\tau \,|\, \boldsymbol{\vartheta})\, g(\boldsymbol{\vartheta})\, \mathrm{d}\boldsymbol{\vartheta}}\, \mathrm{d}\boldsymbol{\theta}, \tag{2.41}$$

where $\int g(\tau \,|\, \boldsymbol{\vartheta})\, g(\boldsymbol{\vartheta})\, \mathrm{d}\boldsymbol{\vartheta} = g(\tau)$. Using Bayes' formula for probability densities,

☞ 430

$$g(\boldsymbol{\theta} \,|\, \tau) = \frac{g(\tau \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})}{g(\tau)}, \tag{2.42}$$

we can write $w_1(\boldsymbol{\theta}) = g(\boldsymbol{\theta} \,|\, \tau)$. With this notation, we have the following definitions.

Definition 2.4: Prior, Likelihood, and Posterior

Let τ and $\mathcal{G}_p := \{g(\cdot \,|\, \boldsymbol{\theta}), \boldsymbol{\theta} \in \boldsymbol{\Theta}\}$ be the training set and family of approximating functions.

PRIOR
- A pdf $g(\boldsymbol{\theta})$ that reflects our *a priori* beliefs about $\boldsymbol{\theta}$ is called the *prior* pdf.

LIKELIHOOD
- The conditional pdf $g(\tau \,|\, \boldsymbol{\theta})$ is called the *likelihood*.

POSTERIOR
- Inference about $\boldsymbol{\theta}$ is given by the *posterior* pdf $g(\boldsymbol{\theta} \,|\, \tau)$, which is proportional to the product of the prior and the likelihood:

$$g(\boldsymbol{\theta} \,|\, \tau) \propto g(\tau \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta}).$$

■ **Remark 2.1 (Early Stopping)** Bayes iteration is an example of an "early stopping" heuristic for maximum likelihood optimization, where we exit after only one step. As observed above, if we keep iterating, we obtain the maximum likelihood estimate (MLE). In a sense the Bayes rule provides a regularization of the MLE. Regularization is discussed in more detail in Chapter 6; see also Example 2.9. The early stopping rule is also of benefit in regularization; see Exercise 20 in Chapter 6. ■

On the one hand, the initial guess $g(\boldsymbol{\theta})$ conveys the *a priori* (prior to training the Bayesian learner) information about the optimal density in $\mathcal{W}_p$ that minimizes the KL risk. Using this prior $g(\boldsymbol{\theta})$, the Bayesian approximation to $f(\boldsymbol{x})$ is the *prior predictive density*:

PRIOR PREDICTIVE DENSITY

$$g(\boldsymbol{x}) = \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})\, \mathrm{d}\boldsymbol{\theta}.$$

On the other hand, the posterior pdf conveys improved knowledge about this optimal density in $\mathcal{W}_p$ after training with τ. Using the posterior $g(\boldsymbol{\theta} \,|\, \tau)$, the Bayesian learner of $f(\boldsymbol{x})$ is the *posterior predictive density*:

POSTERIOR PREDICTIVE DENSITY

$$g_\tau(\boldsymbol{x}) = g(\boldsymbol{x} \,|\, \tau) = \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta} \,|\, \tau)\, \mathrm{d}\boldsymbol{\theta},$$

where we have assumed that $g(\boldsymbol{x} \,|\, \boldsymbol{\theta}, \tau) = g(\boldsymbol{x} \,|\, \boldsymbol{\theta})$; that is, the likelihood depends on τ only through the parameter $\boldsymbol{\theta}$.

The choice of the prior is typically governed by two considerations:

1. the prior should be simple enough to facilitate the computation or simulation of the posterior pdf;
2. the prior should be general enough to model ignorance of the parameter of interest.

Priors that do not convey much knowledge of the parameter are said to be *uninformative*. The uniform or *flat* prior in Example 2.9 (to follow) is frequently used.

UNINFORMATIVE PRIOR

For the purpose of analytical and numerical computations, we can view $\boldsymbol{\theta}$ as a random vector with prior density $g(\boldsymbol{\theta})$, which after training is updated to the posterior density $g(\boldsymbol{\theta} \,|\, \tau)$.

The above thinking allows us to write $g(\boldsymbol{x} \,|\, \tau) \propto \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta})\, g(\tau \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})\, \mathrm{d}\boldsymbol{\theta}$, for example, thus ignoring any constants that do not depend on the argument of the densities.

■ **Example 2.7 (Normal Model)** Suppose that the training data $\mathcal{T} = \{X_1, \ldots, X_n\}$ is modeled using the likelihood $g(x \,|\, \boldsymbol{\theta})$ that is the pdf of

$$X \,|\, \boldsymbol{\theta} \sim \mathcal{N}(\mu, \sigma^2),$$

where $\boldsymbol{\theta} := [\mu, \sigma^2]^\top$. Next, we need to specify the prior distribution of $\boldsymbol{\theta}$ to complete the model. We can specify prior distributions for μ and σ^2 separately and then take their product to obtain the prior for vector $\boldsymbol{\theta}$ (assuming independence). A possible prior distribution for μ is

$$\mu \sim \mathcal{N}(\nu, \phi^2). \tag{2.43}$$

HYPERPARAMETERS

It is typical to refer to any parameters of the prior density as *hyperparameters* of the Bayesian model. Instead of giving directly a prior for σ^2 (or σ), it turns out to be convenient to give the following prior distribution to $1/\sigma^2$:

$$\frac{1}{\sigma^2} \sim \mathsf{Gamma}(\alpha, \beta). \tag{2.44}$$

INVERSE GAMMA

☞ 63

The smaller α and β are, the less informative is the prior. Under this prior, σ^2 is said to have an *inverse gamma*[3] distribution. If $1/Z \sim \mathsf{Gamma}(\alpha, \beta)$, then the pdf of Z is proportional to $\exp(-\beta/z)/z^{\alpha+1}$ (Exercise 19). The Bayesian posterior is then given by:

$$\begin{aligned} g(\mu, \sigma^2 \,|\, \tau) &\propto g(\mu) \times g(\sigma^2) \times g(\tau \,|\, \mu, \sigma^2) \\ &\propto \exp\left\{-\frac{(\mu-\nu)^2}{2\phi^2}\right\} \times \frac{\exp\left\{-\beta/\sigma^2\right\}}{(\sigma^2)^{\alpha+1}} \times \frac{\exp\left\{-\sum_i (x_i-\mu)^2/(2\sigma^2)\right\}}{(\sigma^2)^{n/2}} \\ &\propto (\sigma^2)^{-n/2-\alpha-1} \exp\left\{-\frac{(\mu-\nu)^2}{2\phi^2} - \frac{\beta}{\sigma^2} - \frac{(\mu-\bar{x}_n)^2 + S_n^2}{2\sigma^2/n}\right\}, \end{aligned}$$

where $S_n^2 := \frac{1}{n}\sum_i x_i^2 - \bar{x}_n^2 = \frac{1}{n}\sum_i (x_i - \bar{x}_n)^2$ is the (scaled) sample variance. All inference about (μ, σ^2) is then represented by the posterior pdf. To facilitate computations it is helpful to find out if the posterior belongs to a recognizable family of distributions. For example, the conditional pdf of μ given σ^2 and τ is

$$g(\mu \,|\, \sigma^2, \tau) \propto \exp\left\{-\frac{(\mu-\nu)^2}{2\phi^2} - \frac{(\mu-\bar{x}_n)^2}{2\sigma^2/n}\right\},$$

which after simplification can be recognized as the pdf of

$$(\mu \,|\, \sigma^2, \tau) \sim \mathcal{N}\left(\gamma_n \bar{x}_n + (1-\gamma_n)\nu,\ \gamma_n \sigma^2/n\right), \tag{2.45}$$

where we have defined the weight parameter: $\gamma_n := \frac{n}{\sigma^2} \Big/ \left(\frac{1}{\phi^2} + \frac{n}{\sigma^2}\right)$. We can then see that the posterior mean $\mathbb{E}[\mu \,|\, \sigma^2, \tau] = \gamma_n \bar{x}_n + (1-\gamma_n)\nu$ is a weighted linear combination of the prior mean ν and the sample average $\bar{x}_n$. Further, as $n \to \infty$, the weight $\gamma_n \to 1$ and thus the posterior mean approaches the maximum likelihood estimate $\bar{x}_n$. ■

IMPROPER PRIOR

It is sometimes possible to use a prior $g(\boldsymbol{\theta})$ that is not a *bona fide* probability density, in the sense that $\int g(\boldsymbol{\theta})\, \mathrm{d}\boldsymbol{\theta} = \infty$, as long as the resulting posterior $g(\boldsymbol{\theta} \,|\, \tau) \propto g(\tau \,|\, \boldsymbol{\theta}) g(\boldsymbol{\theta})$ is a proper pdf. Such a prior is called an *improper prior*.

■ **Example 2.8 (Normal Model (cont.))** An example of an improper prior is obtained from (2.43) when we let $\phi \to \infty$ (the larger ϕ is, the more uninformative is the prior). Then, $g(\mu) \propto 1$ is a flat prior, but $\int g(\mu)\, \mathrm{d}\mu = \infty$, making it an improper prior. Nevertheless, the posterior is a proper density, and in particular the conditional posterior of $(\mu \,|\, \sigma^2, \tau)$ simplifies to

$$(\mu \,|\, \sigma^2, \tau) \sim \mathcal{N}\left(\bar{x}_n, \sigma^2/n\right),$$

[3] Reciprocal gamma distribution would have been a better name.

because the weight parameter γ_n goes to 1 as $\phi \to \infty$. The improper prior $g(\mu) \propto 1$ also allows us to simplify the posterior marginal for σ^2:

$$g(\sigma^2 \,|\, \tau) = \int g(\mu, \sigma^2 \,|\, \tau)\, \mathrm{d}\mu \propto (\sigma^2)^{-(n-1)/2-\alpha-1} \exp\left\{-\frac{\beta + nS_n^2/2}{\sigma^2}\right\},$$

which we recognize as the density corresponding to

$$\frac{1}{\sigma^2} \,\Big|\, \tau \sim \mathsf{Gamma}\left(\alpha + \frac{n-1}{2},\, \beta + \frac{n}{2} S_n^2\right).$$

In addition to $g(\mu) \propto 1$, we can also use an improper prior for σ^2. If we take the limit $\alpha \to 0$ and $\beta \to 0$ in (2.44), then we also obtain the improper prior $g(\sigma^2) \propto 1/\sigma^2$ (or equivalently $g(1/\sigma^2) \propto 1/\sigma^2$). In this case, the posterior marginal density for σ^2 implies that:

$$\frac{nS_n^2}{\sigma^2} \,\Big|\, \tau \sim \chi^2_{n-1}$$

and the posterior marginal density for μ implies that:

$$\frac{\mu - \bar{x}_n}{S_n/\sqrt{n-1}} \,\Big|\, \tau \sim \mathsf{t}_{n-1}. \tag{2.46}$$

In general, deriving a simple formula for the posterior density of $\boldsymbol{\theta}$ is either impossible or too tedious. Instead, the Monte Carlo methods in Chapter 3 can be used to simulate (approximately) from the posterior for the purposes of inference and prediction. ■

One way in which a distributional result such as (2.46) can be useful is in the construction of a 95% *credible interval* $\mathcal{I}$ for the parameter μ; that is, an interval $\mathcal{I}$ such that the probability $\mathbb{P}[\mu \in \mathcal{I} \,|\, \tau]$ is equal to 0.95. For example, the symmetric 95% credible interval is

CREDIBLE INTERVAL

$$\mathcal{I} = \left[\bar{x}_n - \frac{S_n}{\sqrt{n-1}}\gamma,\ \bar{x}_n + \frac{S_n}{\sqrt{n-1}}\gamma\right],$$

where γ is the 0.975-quantile of the t_{n-1} distribution. Note that the credible interval is not a random object and that the parameter μ is interpreted as a random variable with a distribution. This is unlike the case of classical confidence intervals, where the parameter is nonrandom, but the interval is (the outcome of) a random object. ☞ 459

As a generalization of the 95% Bayesian credible interval we can define a $1-\alpha$ *credible region*, which is any set $\mathcal{R}$ satisfying

CREDIBLE REGION

$$\mathbb{P}[\boldsymbol{\theta} \in \mathcal{R} \,|\, \tau] = \int_{\boldsymbol{\theta} \in \mathcal{R}} g(\boldsymbol{\theta} \,|\, \tau)\, \mathrm{d}\boldsymbol{\theta} \geqslant 1 - \alpha. \tag{2.47}$$

■ **Example 2.9 (Bayesian Regularization of Maximum Likelihood)** Consider modeling the number of deaths during birth in a maternity ward. Suppose that the hospital data consists of $\tau = \{x_1, \ldots, x_n\}$, with $x_i = 1$ if the i-th baby has died during birth and $x_i = 0$ otherwise, for $i = 1, \ldots, n$. A possible Bayesian model for the data is $\theta \sim \mathcal{U}(0,1)$ (uniform prior) with $(X_1, \ldots, X_n \,|\, \theta) \overset{\text{iid}}{\sim} \mathsf{Ber}(\theta)$. The likelihood is therefore

$$g(\tau \,|\, \theta) = \prod_{i=1}^{n} \theta^{x_i} (1-\theta)^{1-x_i} = \theta^s \, (1-\theta)^{n-s},$$

where $s = x_1 + \cdots + x_n$ is the total number of deaths. Since $g(\theta) = 1$, the posterior pdf is

$$g(\theta \,|\, \tau) \propto \theta^s \, (1-\theta)^{n-s}, \quad \theta \in [0,1],$$

which is the pdf of the $\mathsf{Beta}(s+1, n-s+1)$ distribution. The normalization constant is $(n+1)\binom{n}{s}$. The posterior pdf is shown in Figure 2.14 for $(s,n) = (0,100)$. It is not difficult

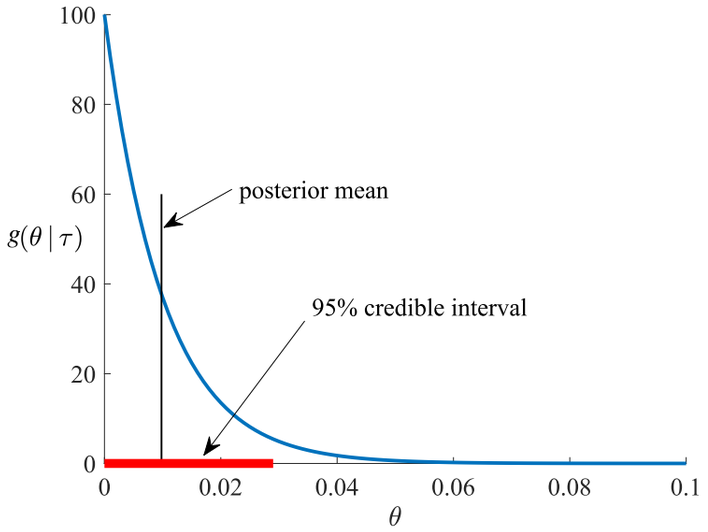


Figure 2.14: Posterior pdf for θ, with $n = 100$ and $s = 0$.

MAXIMUM A POSTERIORI

to see that the *maximum a posteriori* (MAP) estimate of θ (the mode or maximizer of the posterior density) is

$$\underset{\theta}{\text{argmax}}\, g(\theta \,|\, \tau) = \frac{s}{n},$$

which agrees with the maximum likelihood estimate. Figure 2.14 also shows that the left one-sided 95% credible interval for θ is $[0, 0.0292]$, where 0.0292 is the 0.95 quantile (rounded) of the $\mathsf{Beta}(1, 101)$ distribution.

Observe that when $(s,n) = (0,100)$ the maximum likelihood estimate $\widehat{\theta} = 0$ infers that deaths at birth are not possible. We know that this inference is wrong — the probability of death can never be zero, it is simply (and fortunately) too small to be inferred accurately from a sample size of $n = 100$. In contrast to the maximum likelihood estimate, the posterior mean $\mathbb{E}[\theta \,|\, \tau] = (s+1)/(n+2)$ is not zero for $(s,n) = (0,100)$ and provides the more reasonable point estimate of 0.0098 for the probability of death.

In addition, while computing a Bayesian credible interval poses no conceptual difficulties, it is not simple to derive a confidence interval for the maximum likelihood estimate of $\widehat{\theta}$, because the likelihood as a function of θ is not differentiable at $\theta = 0$. As a result of this lack of smoothness, the usual confidence intervals based on the normal approximation cannot be used. ■

We now return to the unsupervised learning setting of Section 2.6, but consider this from a Bayesian perspective. Recall from (2.39) that the Kullback–Leibler risk for an approximating function g is

$$\ell(g) = \int f(\tau'_n)[\ln f(\tau'_n) - \ln g(\tau'_n)]\,\mathrm{d}\tau'_n,$$

where τ'_n denotes the test data. Since $\int f(\tau'_n) \ln f(\tau'_n)\,\mathrm{d}\tau'_n$ plays no role in minimizing the risk, we consider instead the *cross-entropy risk*, defined as ☞ 122

$$\ell(g) = -\int f(\tau'_n) \ln g(\tau'_n)\,\mathrm{d}\tau'_n.$$

Note that the smallest possible cross-entropy risk is $\ell_n^* = -\int f(\tau'_n) \ln f(\tau'_n)\,\mathrm{d}\tau'_n$. The expected generalization risk of the Bayesian learner can then be decomposed as

$$\mathbb{E}\,\ell(g_{\mathcal{T}_n}) = \ell_n^* + \underbrace{\int f(\tau'_n) \ln \frac{f(\tau'_n)}{\mathbb{E}\,g(\tau'_n \,|\, \mathcal{T}_n)}\,\mathrm{d}\tau'_n}_{\text{“bias” component}} + \underbrace{\mathbb{E} \int f(\tau'_n) \ln \frac{\mathbb{E}\,g(\tau'_n \,|\, \mathcal{T}_n)}{g(\tau'_n \,|\, \mathcal{T}_n)}\,\mathrm{d}\tau'_n}_{\text{“variance” component}},$$

where $g_{\mathcal{T}_n}(\tau'_n) = g(\tau'_n \,|\, \mathcal{T}_n) = \int g(\tau'_n \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta} \,|\, \mathcal{T}_n)\,\mathrm{d}\boldsymbol{\theta}$ is the posterior predictive density after observing $\mathcal{T}_n$.

Assuming that the sets $\mathcal{T}_n$ and $\mathcal{T}'_n$ are comprised of $2n$ iid random variables with density f, we can show (Exercise 23) that the expected generalization risk simplifies to

$$\mathbb{E}\,\ell(g_{\mathcal{T}_n}) = \mathbb{E} \ln g(\mathcal{T}_n) - \mathbb{E} \ln g(\mathcal{T}_{2n}), \tag{2.48}$$

where $g(\tau_n)$ and $g(\tau_{2n})$ are the prior predictive densities of τ_n and τ_{2n}, respectively.

Let $\overline{\boldsymbol{\theta}}_n = \operatorname{argmax}_{\boldsymbol{\theta}} g(\boldsymbol{\theta} \,|\, \mathcal{T}_n)$ be the MAP estimator of $\boldsymbol{\theta}^* := \operatorname{argmax}_{\boldsymbol{\theta}} \mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})$. Assuming that $\overline{\boldsymbol{\theta}}_n$ converges to $\boldsymbol{\theta}^*$ (with probability one) and $\frac{1}{n}\mathbb{E} \ln g(\mathcal{T}_n \,|\, \overline{\boldsymbol{\theta}}_n) = \mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}^*) + O(1/n)$, we can use the following large-sample approximation of the expected generalization risk.

Theorem 2.4: Approximating the Bayesian Cross-Entropy Risk

For $n \to \infty$, the expected cross-entropy generalization risk satisfies:

$$\mathbb{E}\ell(g_{\mathcal{T}_n}) \simeq -\mathbb{E} \ln g(\mathcal{T}_n) - \frac{p}{2} \ln n, \tag{2.49}$$

where (with p the dimension of the parameter vector $\boldsymbol{\theta}$ and $\overline{\boldsymbol{\theta}}_n$ the MAP estimator):

$$\mathbb{E} \ln g(\mathcal{T}_n) \simeq \mathbb{E} \ln g(\mathcal{T}_n \,|\, \overline{\boldsymbol{\theta}}_n) - \frac{p}{2} \ln n. \tag{2.50}$$

☞ 452

Proof: To show (2.50), we apply Theorem C.21 to $\ln \int \mathrm{e}^{-nr_n(\boldsymbol{\theta})} g(\boldsymbol{\theta})\,\mathrm{d}\boldsymbol{\theta}$, where

$$r_n(\boldsymbol{\theta}) := -\frac{1}{n} \ln g(\mathcal{T}_n \,|\, \boldsymbol{\theta}) = -\frac{1}{n} \sum_{i=1}^{n} \ln g(\boldsymbol{X}_i \,|\, \boldsymbol{\theta}) \xrightarrow{\text{a.s.}} -\mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}) =: r(\boldsymbol{\theta}) < \infty.$$

This gives (with probability one)

$$\ln \int g(\mathcal{T}_n \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})\,\mathrm{d}\boldsymbol{\theta} \simeq -nr(\boldsymbol{\theta}^*) - \frac{p}{2} \ln(n).$$

Taking expectations on both sides and using $nr(\boldsymbol{\theta}^*) = n\mathbb{E}[r_n(\overline{\boldsymbol{\theta}}_n)] + O(1)$, we deduce (2.50). To demonstrate (2.49), we derive the asymptotic approximation of $\mathbb{E} \ln g(\mathcal{T}_{2n})$ by repeating the argument for (2.50), but replacing n with $2n$, where necessary. Thus, we obtain:

$$\mathbb{E} \ln g(\mathcal{T}_{2n}) \simeq -2nr(\boldsymbol{\theta}^*) - \frac{p}{2} \ln(2n).$$

Then, (2.49) follows from the identity (2.48). □

The results of Theorem 2.4 have two major implications for model selection and assessment. First, (2.49) suggests that $-\ln g(\mathcal{T}_n)$ can be used as a crude (leading-order) asymptotic approximation to the expected generalization risk for large n and fixed p. In this context, the prior predictive density $g(\mathcal{T}_n)$ is usually called the *model evidence* or *marginal likelihood* for the class $\mathcal{G}_p$. Since the integral $\int g(\mathcal{T}_n \,|\, \boldsymbol{\theta})\, g(\boldsymbol{\theta})\,\mathrm{d}\boldsymbol{\theta}$ is rarely available in closed form, the exact computation of the model evidence is typically not feasible and may require Monte Carlo estimation methods.

MODEL EVIDENCE

☞ 78

Second, when the model evidence is difficult to compute via Monte Carlo methods or otherwise, (2.50) suggests that we can use the following large-sample approximation:

$$-2\mathbb{E} \ln g(\mathcal{T}_n) \simeq -2 \ln g(\mathcal{T}_n \,|\, \overline{\boldsymbol{\theta}}_n) + p \ln(n). \tag{2.51}$$

The asymptotic approximation on the right-hand side of (2.51) is called the *Bayesian information criterion* (BIC). We prefer the class $\mathcal{G}_p$ with the smallest BIC. The BIC is typically used when the model evidence is difficult to compute and n is sufficiently larger than p. For a fixed p, and as n becomes larger and larger, the BIC becomes a more and more accurate estimator of $-2\mathbb{E} \ln g(\mathcal{T}_n)$. Note that the BIC approximation is valid even when the true density $f \notin \mathcal{G}_p$. The BIC provides an alternative to the *Akaike information criterion* (AIC) for model selection. However, while the BIC approximation does not assume that the true model f belongs to the parametric class under consideration, the AIC assumes that $f \in \mathcal{G}_p$. Thus, the AIC is merely a *heuristic* approximation based on the asymptotic approximations in Theorem 4.1.

BAYESIAN INFORMATION CRITERION

☞ 126

Although the above Bayesian theory has been presented in an unsupervised learning setting, it can be readily extended to the supervised case. We only need to relabel the training set $\mathcal{T}_n$. In particular, when (as is typical for regression models) the training responses $Y_1, \ldots, Y_n$ are considered as random variables but the corresponding feature vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are viewed as being fixed, then $\mathcal{T}_n$ is the collection of random responses $\{Y_1, \ldots, Y_n\}$. Alternatively, we can simply identify $\mathcal{T}_n$ with the response vector $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$. We will adopt this notation in the next example.

■ **Example 2.10 (Polynomial Regression (cont.))** Consider Example 2.2 once again, but now in a Bayesian framework, where the prior knowledge on $(\sigma^2, \boldsymbol{\beta})$ is specified by $g(\sigma^2) = 1/\sigma^2$ and $\boldsymbol{\beta} \,|\, \sigma^2 \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{D})$, and $\mathbf{D}$ is a (matrix) hyperparameter. Let $\boldsymbol{\Sigma} := (\mathbf{X}^\top \mathbf{X} + \mathbf{D}^{-1})^{-1}$. Then the posterior can be written as:

$$\begin{aligned} g(\boldsymbol{\beta}, \sigma^2 \,|\, \boldsymbol{y}) &= \frac{\exp\left(-\frac{\|\boldsymbol{y}-\mathbf{X}\boldsymbol{\beta}\|^2}{2\sigma^2}\right)}{(2\pi\sigma^2)^{n/2}} \times \frac{\exp\left(-\frac{\boldsymbol{\beta}^\top \mathbf{D}^{-1}\boldsymbol{\beta}}{2\sigma^2}\right)}{(2\pi\sigma^2)^{p/2}\,|\mathbf{D}|^{1/2}} \times \frac{1}{\sigma^2} \Big/ g(\boldsymbol{y}) \\ &= \frac{(\sigma^2)^{-(n+p)/2-1}}{(2\pi)^{(n+p)/2}\,|\mathbf{D}|^{1/2}} \exp\left(-\frac{\|\Sigma^{-1/2}(\boldsymbol{\beta}-\overline{\boldsymbol{\beta}})\|^2}{2\sigma^2} - \frac{(n+p+2)\,\overline{\sigma}^2}{2\sigma^2}\right) \Big/ g(\boldsymbol{y}), \end{aligned}$$

where $\overline{\boldsymbol{\beta}} := \boldsymbol{\Sigma}\mathbf{X}^\top \boldsymbol{y}$ and $\overline{\sigma}^2 := \boldsymbol{y}^\top(\mathbf{I} - \mathbf{X}\boldsymbol{\Sigma}\mathbf{X}^\top)\boldsymbol{y}/(n+p+2)$ are the MAP estimates of $\boldsymbol{\beta}$ and σ^2, and $g(\boldsymbol{y})$ is the model evidence for $\mathcal{G}_p$:

$$\begin{aligned} g(\boldsymbol{y}) &= \iint g(\boldsymbol{\beta}, \sigma^2, \boldsymbol{y})\, \mathrm{d}\boldsymbol{\beta}\, \mathrm{d}\sigma^2 \\ &= \frac{|\boldsymbol{\Sigma}|^{1/2}}{(2\pi)^{n/2}|\mathbf{D}|^{1/2}} \int_0^\infty \frac{\exp\left(-\frac{(n+p+2)\,\overline{\sigma}^2}{2\sigma^2}\right)}{(\sigma^2)^{n/2+1}}\, \mathrm{d}\sigma^2 \\ &= \frac{|\boldsymbol{\Sigma}|^{1/2}\Gamma(n/2)}{|\mathbf{D}|^{1/2}(\pi(n+p+2)\,\overline{\sigma}^2)^{n/2}}. \end{aligned}$$

Therefore, based on (2.49), we have

$$2\mathbb{E}\ell(g_{\mathcal{T}_n}) \simeq -2\ln g(\boldsymbol{y}) = n\ln\left[\pi(n+p+2)\,\overline{\sigma}^2\right] - 2\ln\Gamma(n/2) + \ln|\mathbf{D}| - \ln|\boldsymbol{\Sigma}|.$$

On the other hand, the minus of the log-likelihood of $\boldsymbol{Y}$ can be written as

$$\begin{aligned} -\ln g(\boldsymbol{y} \,|\, \boldsymbol{\beta}, \sigma^2) &= \frac{\|\boldsymbol{y}-\mathbf{X}\boldsymbol{\beta}\|^2}{2\sigma^2} + \frac{n}{2}\ln(2\pi\sigma^2) \\ &= \frac{\|\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{\beta}-\overline{\boldsymbol{\beta}})\|^2}{2\sigma^2} + \frac{(n+p+2)\,\overline{\sigma}^2}{2\sigma^2} + \frac{n}{2}\ln(2\pi\sigma^2). \end{aligned}$$

Therefore, the BIC approximation (2.51) is

$$-2\ln g(\boldsymbol{y} \,|\, \overline{\boldsymbol{\beta}}, \overline{\sigma}^2) + (p+1)\ln(n) = n[\ln(2\pi\,\overline{\sigma}^2) + 1] + (p+1)\ln(n) + (p+2), \qquad (2.52)$$

where the extra $\ln(n)$ term in $(p+1)\ln(n)$ is due to the inclusion of σ^2 in $\boldsymbol{\theta} = (\sigma^2, \boldsymbol{\beta})$. Figure 2.15 shows the model evidence and its BIC approximation, where we used a hyperparameter $\mathbf{D} = 10^4 \times \mathbf{I}_p$ for the prior density of $\boldsymbol{\beta}$. We can see that both approximations exhibit a pronounced minimum at $p = 4$, thus identifying the true polynomial regression model. Compare the overall qualitative shape of the cross-entropy risk estimate with the shape of the square-error risk estimate in Figure 2.11.

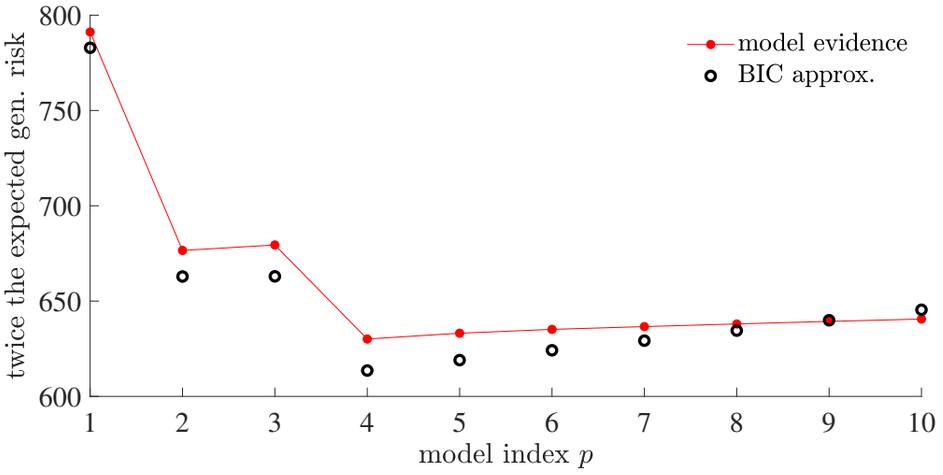


Figure 2.15: The BIC and marginal likelihood used for model selection.

■

It is possible to give the model complexity parameter p a Bayesian treatment, in which we define a prior density on the set of all models under consideration. For example, let $g(p)$, $p = 1, \ldots, m$ be a prior density on m candidate models. Treating the model complexity index p as an additional parameter to $\boldsymbol{\theta} \in \mathbb{R}^p$, and applying Bayes' formula, the posterior for $(\boldsymbol{\theta}, p)$ can be written as:

$$\begin{aligned} g(\boldsymbol{\theta}, p \,|\, \tau) &= g(\boldsymbol{\theta} \,|\, p, \tau) \times g(p \,|\, \tau) \\ &= \underbrace{\frac{g(\tau \,|\, \boldsymbol{\theta}, p)\, g(\boldsymbol{\theta} \,|\, p)}{g(\tau \,|\, p)}}_{\text{posterior of } \boldsymbol{\theta} \text{ given model } p} \times \underbrace{\frac{g(\tau \,|\, p)\, g(p)}{g(\tau)}}_{\text{posterior of model } p}. \end{aligned}$$

The model evidence for a fixed p is now interpreted as the prior predictive density of τ, conditional on the model p:

$$g(\tau \,|\, p) = \int g(\tau \,|\, \boldsymbol{\theta}, p)\, g(\boldsymbol{\theta} \,|\, p)\, \mathrm{d}\boldsymbol{\theta},$$

and the quantity $g(\tau) = \sum_{p=1}^{m} g(\tau \,|\, p)\, g(p)$ is interpreted as the marginal likelihood of all the m candidate models. Finally, a simple method for model selection is to pick the index $\widehat{p}$ with the largest posterior probability:

$$\widehat{p} = \operatorname*{argmax}_p g(p \,|\, \tau) = \operatorname*{argmax}_p g(\tau \,|\, p)\, g(p).$$

■ **Example 2.11 (Polynomial Regression (cont.))** Let us revisit Example 2.10 by giving the parameter $p = 1, \ldots, m$, with $m = 10$, a Bayesian treatment. Recall that we used the notation $\tau = \boldsymbol{y}$ in that example. We assume that the prior $g(p) = 1/m$ is flat and uninformative so that the posterior is given by

$$g(p \,|\, \boldsymbol{y}) \propto g(\boldsymbol{y} \,|\, p) = \frac{|\boldsymbol{\Sigma}|^{1/2}\, \Gamma(n/2)}{|\mathbf{D}|^{1/2} (\pi(n + p + 2)\, \overline{\sigma}^2)^{n/2}},$$

where all quantities in $g(\mathbf{y} \mid p)$ are computed using the first p columns of $\mathbf{X}$. Figure 2.16 shows the resulting posterior density $g(p \mid \mathbf{y})$. The figure also shows the posterior density $\widehat{g}(\mathbf{y} \mid p) / \sum_{p=1}^{10} \widehat{g}(\mathbf{y} \mid p)$, where

$$\widehat{g}(\mathbf{y} \mid p) := \exp\left(-\frac{n[\ln(2\pi\,\overline{\sigma}^2) + 1] + (p+1)\ln(n) + (p+2)}{2}\right)$$

is derived from the BIC approximation (2.52). In both cases, there is a clear maximum at $p = 4$, suggesting that a third-degree polynomial is the most appropriate model for the data.

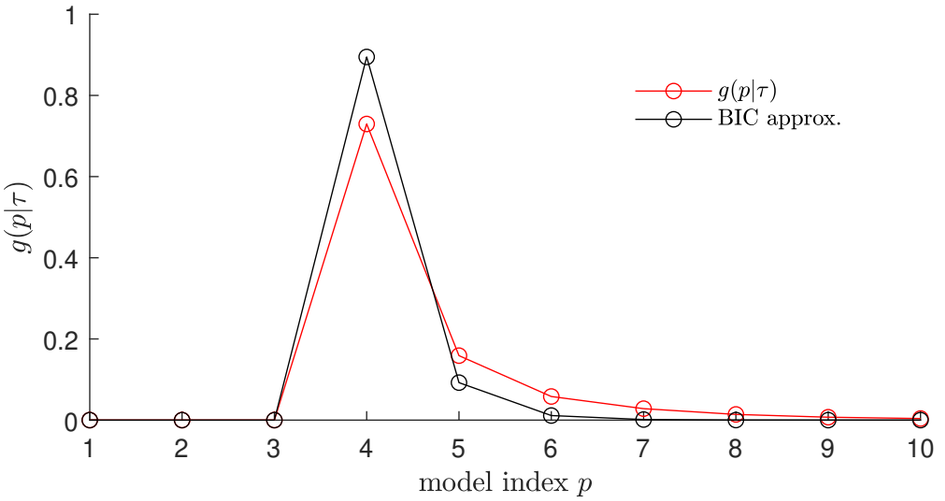


Figure 2.16: Posterior probabilities for each polynomial model of degree $p - 1$.

■

Suppose that we wish to compare two models, say model $p = 1$ and model $p = 2$. Instead of computing the posterior $g(p \mid \tau)$ explicitly, we can compare the posterior odds ratio:

$$\frac{g(p=1 \mid \tau)}{g(p=2 \mid \tau)} = \frac{g(p=1)}{g(p=2)} \times \underbrace{\frac{g(\tau \mid p=1)}{g(\tau \mid p=2)}}_{\text{Bayes factor } B_{1\mid 2}}.$$

This gives rise to the *Bayes factor* $B_{i\mid j}$, whose value signifies the strength of the evidence in favor of model i over model j. In particular $B_{i\mid j} > 1$ means that the evidence in favor for model i is larger. BAYES FACTOR

■ **Example 2.12 (Savage–Dickey Ratio)** Suppose that we have two models. Model $p = 2$ has a likelihood $g(\tau \mid \mu, \nu, p = 2)$, depending on two parameters. Model $p = 1$ has the same functional form for the likelihood but now ν is fixed to some (known) ν_0; that is, $g(\tau \mid \mu, p = 1) = g(\tau \mid \mu, \nu = \nu_0, p = 2)$. We also assume that the prior information on μ

for model 1 is the same as that for model 2, conditioned on $\nu = \nu_0$. That is, we assume $g(\mu \,|\, p = 1) = g(\mu \,|\, \nu = \nu_0, p = 2)$. As model 2 contains model 1 as a special case, the latter is said to be *nested* inside model 2. We can formally write (see also Exercise 26):

$$\begin{aligned} g(\tau \,|\, p = 1) &= \int g(\tau \,|\, \mu, p = 1)\, g(\mu \,|\, p = 1)\, \mathrm{d}\mu \\ &= \int g(\tau \,|\, \mu, \nu = \nu_0, p = 2)\, g(\mu \,|\, \nu = \nu_0, p = 2)\, \mathrm{d}\mu \\ &= g(\tau \,|\, \nu = \nu_0, p = 2) = \frac{g(\tau, \nu = \nu_0 \,|\, p = 2)}{g(\nu = \nu_0 \,|\, p = 2)}. \end{aligned}$$

Hence, the Bayes factor simplifies to

$$B_{1|2} = \frac{g(\tau \,|\, p = 1)}{g(\tau \,|\, p = 2)} = \frac{g(\tau, \nu = \nu_0 \,|\, p = 2)}{g(\nu = \nu_0 \,|\, p = 2)} \Big/ g(\tau \,|\, p = 2) = \frac{g(\nu = \nu_0 \,|\, \tau, p = 2)}{g(\nu = \nu_0 \,|\, p = 2)}.$$

In other words, $B_{1|2}$ is the ratio of the posterior density to the prior density of ν, evaluated at $\nu = \nu_0$ and both under the unrestricted model $p = 2$. This ratio of posterior to prior densities is called the *Savage–Dickey density ratio*. ■

SAVAGE–DICKEY DENSITY RATIO

Whether to use a classical (frequentist) or Bayesian model is largely a question of convenience. Classical inference is useful because it comes with a huge repository of ready-to-use results, and requires no (subjective) prior information on the parameters. Bayesian models are useful because the whole theory is based on the elegant Bayes' formula, and uncertainty in the inference (e.g., confidence intervals) can be quantified much more naturally (e.g., credible intervals). A usual practice is to "Bayesify" a classical model, simply by adding some prior information on the parameters.

Further Reading

A popular textbook on statistical learning is [55]. Accessible treatments of mathematical statistics can be found, for example, in [69], [74], and [124]. More advanced treatments are given in [10], [25], and [78]. A good overview of modern-day statistical inference is given in [36]. Classical references on pattern classification and machine learning are [12] and [35]. For advanced learning theory including information theory and Rademacher complexity, we refer to [28] and [109]. An applied reference for Bayesian inference is [46]. For a survey of numerical techniques relevant to computational statistics, see [90].

Exercises

1. Suppose that the loss function is the piecewise linear function

$$\mathrm{Loss}(y, \widehat{y}) = \alpha\, (\widehat{y} - y)_+ + \beta\, (y - \widehat{y})_+, \quad \alpha, \beta > 0,$$

where c_+ is equal to c if $c > 0$, and zero otherwise. Show that the minimizer of the risk $\ell(g) = \mathbb{E}\,\mathrm{Loss}(Y, g(\boldsymbol{X}))$ satisfies

$$\mathbb{P}[Y < g^*(\boldsymbol{x}) \,|\, \boldsymbol{X} = \boldsymbol{x}] = \frac{\beta}{\alpha + \beta}.$$

In other words, $g^*(\boldsymbol{x})$ is the $\beta/(\alpha + \beta)$ quantile of Y, conditional on $\boldsymbol{X} = \boldsymbol{x}$.

2. Show that, for the squared-error loss, the approximation error $\ell(g^{\mathcal{G}}) - \ell(g^*)$ in (2.16), is equal to $\mathbb{E}(g^{\mathcal{G}}(\boldsymbol{X}) - g^*(\boldsymbol{X}))^2$. [Hint: expand $\ell(g^{\mathcal{G}}) = \mathbb{E}(Y - g^*(\boldsymbol{X}) + g^*(\boldsymbol{X}) - g^{\mathcal{G}}(\boldsymbol{X}))^2$.]

3. Suppose $\mathcal{G}$ is the class of *linear* functions. A linear function evaluated at a feature $\boldsymbol{x}$ can be described as $g(\boldsymbol{x}) = \boldsymbol{\beta}^\top \boldsymbol{x}$ for some parameter vector $\boldsymbol{\beta}$ of appropriate dimension. Denote $g^{\mathcal{G}}(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta}^{\mathcal{G}}$ and $g_\tau^{\mathcal{G}}(\boldsymbol{x}) = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}$. Show that

$$\mathbb{E}\left(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - g^*(\boldsymbol{X})\right)^2 = \mathbb{E}\left(\boldsymbol{X}^\top \widehat{\boldsymbol{\beta}} - \boldsymbol{X}^\top \boldsymbol{\beta}^{\mathcal{G}}\right)^2 + \mathbb{E}\left(\boldsymbol{X}^\top \boldsymbol{\beta}^{\mathcal{G}} - g^*(\boldsymbol{X})\right)^2.$$

Hence, deduce that the statistical error in (2.16) is $\ell(g_\tau^{\mathcal{G}}) - \ell(g^{\mathcal{G}}) = \mathbb{E}\,(g_\tau^{\mathcal{G}}(\boldsymbol{X}) - g^{\mathcal{G}}(\boldsymbol{X}))^2$.

4. Show that formula (2.24) holds for the 0–1 loss with 0–1 response.

5. Let $\boldsymbol{X}$ be an n-dimensional normal random vector with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$, where the determinant of $\boldsymbol{\Sigma}$ is non-zero. Show that $\boldsymbol{X}$ has joint probability density

$$f_{\boldsymbol{X}}(\boldsymbol{x}) = \frac{1}{\sqrt{(2\pi)^n\,|\boldsymbol{\Sigma}|}}\, \mathrm{e}^{-\frac{1}{2}\,(\boldsymbol{x}-\boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{x}-\boldsymbol{\mu})}, \quad \boldsymbol{x} \in \mathbb{R}^n.$$

6. Let $\widehat{\boldsymbol{\beta}} = \mathbf{A}^+ \boldsymbol{y}$. Using the defining properties of the pseudo-inverse, show that for any $\boldsymbol{\beta} \in \mathbb{R}^p$, ☞ 362

$$\|\mathbf{A}\widehat{\boldsymbol{\beta}} - \boldsymbol{y}\| \leqslant \|\mathbf{A}\boldsymbol{\beta} - \boldsymbol{y}\|.$$

7. Suppose that in the polynomial regression Example 2.1 we select the linear class of functions $\mathcal{G}_p$ with $p \geqslant 4$. Then, $g^* \in \mathcal{G}_p$ and the approximation error is zero, because $g^{\mathcal{G}_p}(\boldsymbol{x}) = g^*(\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{\beta}$, where $\boldsymbol{\beta} = [10, -140, 400, -250, 0, \ldots, 0]^\top \in \mathbb{R}^p$. Use the tower property to show that the learner $g_\tau(\boldsymbol{x}) = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}$ with $\widehat{\boldsymbol{\beta}} = \mathbf{X}^+ \boldsymbol{y}$, assuming $\mathrm{rank}(\mathbf{X}) \geqslant 4$, is *unbiased*: ☞ 433 UNBIASED

$$\mathbb{E}\, g_{\mathcal{T}}(\boldsymbol{x}) = g^*(\boldsymbol{x}).$$

8. (Exercise 7 continued.) Observe that the learner $g_{\mathcal{T}}$ can be written as a linear combination of the response variable: $g_{\mathcal{T}}(\boldsymbol{x}) = \boldsymbol{x}^\top \mathbf{X}^+ \boldsymbol{Y}$. Prove that for any learner of the form $\boldsymbol{x}^\top \mathbf{A}\boldsymbol{y}$, where $\mathbf{A} \in \mathbb{R}^{p \times n}$ is some matrix and that satisfies $\mathbb{E}_{\mathbf{X}}[\boldsymbol{x}^\top \mathbf{A}\boldsymbol{Y}] = g^*(\boldsymbol{x})$, we have

$$\mathbb{V}\mathrm{ar}_{\mathbf{X}}[\boldsymbol{x}^\top \mathbf{X}^+ \boldsymbol{Y}] \leqslant \mathbb{V}\mathrm{ar}_{\mathbf{X}}[\boldsymbol{x}^\top \mathbf{A}\boldsymbol{Y}],$$

where the equality is achieved for $\mathbf{A} = \mathbf{X}^+$. This is called the *Gauss–Markov inequality*. Hence, using the Gauss–Markov inequality deduce that for the unconditional variance: GAUSS–MARKOV INEQUALITY

$$\mathbb{V}\mathrm{ar}\, g_{\mathcal{T}}(\boldsymbol{x}) \leqslant \mathbb{V}\mathrm{ar}[\boldsymbol{x}^\top \mathbf{A}\boldsymbol{Y}].$$

Deduce that $\mathbf{A} = \mathbf{X}^+$ also minimizes the expected generalization risk.

9. Consider again the polynomial regression Example 2.1. Use the fact that $\mathbb{E}_{\mathbf{X}}\, \widehat{\boldsymbol{\beta}} = \mathbf{X}^+ \boldsymbol{h}^*(\boldsymbol{u})$, where $\boldsymbol{h}^*(\boldsymbol{u}) = \mathbb{E}[\boldsymbol{Y} \,|\, \boldsymbol{U} = \boldsymbol{u}] = [h^*(u_1), \ldots, h^*(u_n)]^\top$, to show that the expected in-sample risk is:

$$\mathbb{E}_{\mathbf{X}}\, \ell_{\mathrm{in}}(g_{\mathcal{T}}) = \ell^* + \frac{\|\boldsymbol{h}^*(\boldsymbol{u})\|^2 - \|\mathbf{X}\mathbf{X}^+ \boldsymbol{h}^*(\boldsymbol{u})\|^2}{n} + \frac{\ell^* p}{n}.$$

Also, use Theorem C.2 to show that the expected statistical error is: ☞ 432

$$\mathbb{E}_{\mathbf{X}}\, (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta})^\top \mathbf{H}_p (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}) = \ell^* \mathrm{tr}(\mathbf{X}^+ (\mathbf{X}^+)^\top \mathbf{H}_p) + (\mathbf{X}^+ \boldsymbol{h}^*(\boldsymbol{u}) - \boldsymbol{\beta})^\top \mathbf{H}_p (\mathbf{X}^+ \boldsymbol{h}^*(\boldsymbol{u}) - \boldsymbol{\beta}).$$

10. Consider the setting of the polynomial regression in Example 2.2. Use Theorem C.19 to prove that

☞ 451

$$\sqrt{n}\,(\widehat{\boldsymbol{\beta}}_n - \boldsymbol{\beta}_p) \xrightarrow{\mathrm{d}} \mathcal{N}\Big(\mathbf{0},\, \ell^* \mathbf{H}_p^{-1} + \mathbf{H}_p^{-1}\mathbf{M}_p\mathbf{H}_p^{-1}\Big), \tag{2.53}$$

where $\mathbf{M}_p := \mathbb{E}[\boldsymbol{X}\boldsymbol{X}^\top (g^*(\boldsymbol{X}) - g^{\mathcal{G}_p}(\boldsymbol{X}))^2]$ is the matrix with (i,j)-th entry:

$$\int_0^1 u^{i+j-2} (h^{\mathcal{H}_p}(u) - h^*(u))^2 \,\mathrm{d}u,$$

INVERSE HILBERT MATRIX

and $\mathbf{H}_p^{-1}$ is the $p \times p$ *inverse Hilbert matrix* with (i,j)-th entry:

$$(-1)^{i+j}(i+j-1)\binom{p+i-1}{p-j}\binom{p+j-1}{p-i}\binom{i+j-2}{i-1}^2.$$

Observe that $\mathbf{M}_p = \mathbf{0}$ for $p \geqslant 4$, so that the matrix $\mathbf{M}_p$ term is due to choosing a restrictive class $\mathcal{G}_p$ that does not contain the true prediction function.

11. In Example 2.2 we saw that the statistical error can be expressed (see (2.20)) as

$$\int_0^1 \Big([1, \ldots, u^{p-1}](\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p)\Big)^2 \,\mathrm{d}u = (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p)^\top \mathbf{H}_p (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p).$$

By Exercise 10 the random vector $\boldsymbol{Z}_n := \sqrt{n}(\widehat{\boldsymbol{\beta}}_n - \boldsymbol{\beta}_p)$ has asymptotically a multivariate normal distribution with mean vector $\mathbf{0}$ and covariance matrix $\mathbf{V} := \ell^* \mathbf{H}_p^{-1} + \mathbf{H}_p^{-1}\mathbf{M}_p\mathbf{H}_p^{-1}$. Use Theorem C.2 to show that the *expected* statistical error is asymptotically

☞ 432

$$\mathbb{E}\,(\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p)^\top \mathbf{H}_p (\widehat{\boldsymbol{\beta}} - \boldsymbol{\beta}_p) \simeq \frac{\ell^* p}{n} + \frac{\mathrm{tr}(\mathbf{M}_p \mathbf{H}_p^{-1})}{n}, \quad n \to \infty. \tag{2.54}$$

Plot this large-sample approximation of the expected statistical error and compare it with the outcome of the statistical error.

We note a subtle technical detail: In general, convergence in distribution does not imply convergence in L_p-norm (see Example C.6), and so here we have implicitly assumed that $\|\boldsymbol{Z}_n\| \xrightarrow{\mathrm{d}} \mathsf{Dist.} \Rightarrow \|\boldsymbol{Z}_n\| \xrightarrow{L_2} \text{constant} := \lim_{n\uparrow\infty} \mathbb{E}\|\boldsymbol{Z}_n\|$.

☞ 444

12. Consider again Example 2.2. The result in (2.53) suggests that $\mathbb{E}\widehat{\boldsymbol{\beta}} \to \boldsymbol{\beta}_p$ as $n \to \infty$, where $\boldsymbol{\beta}_p$ is the solution in the class $\mathcal{G}_p$ given in (2.18). Thus, the large-sample approximation of the pointwise bias of the learner $g_{\mathcal{T}}^{\mathcal{G}_p}(\boldsymbol{x}) = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}$ at $\boldsymbol{x} = [1, \ldots, u^{p-1}]^\top$ is

$$\mathbb{E}\, g_{\mathcal{T}}^{\mathcal{G}_p}(\boldsymbol{x}) - g^*(\boldsymbol{x}) \simeq [1, \ldots, u^{p-1}]\boldsymbol{\beta}_p - [1, u, u^2, u^3]\boldsymbol{\beta}^*, \quad n \to \infty.$$

Use Python to reproduce Figure 2.17, which shows the (large-sample) pointwise squared bias of the learner for $p \in \{1, 2, 3\}$. Note how the bias is larger near the endpoints $u = 0$ and $u = 1$. Explain why the areas under the curves correspond to the approximation errors.

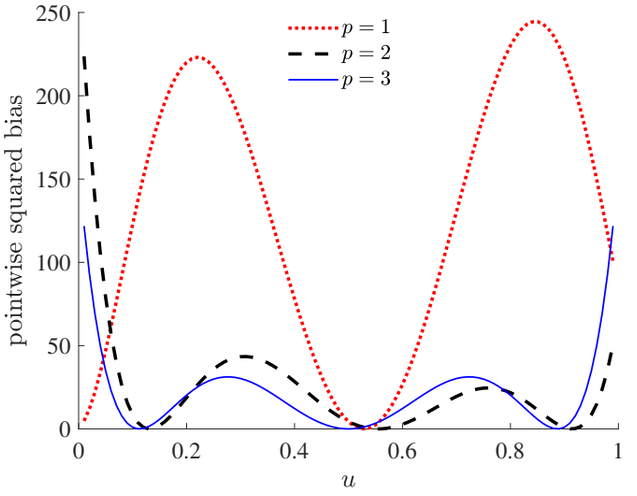


Figure 2.17: The large-sample pointwise squared bias of the learner for $p = 1, 2, 3$. The bias is zero for $p \geqslant 4$.

13. For our running Example 2.2 we can use (2.53) to derive a large-sample approximation of the pointwise variance of the learner $g_{\mathcal{T}}(\boldsymbol{x}) = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}_n$. In particular, show that for large n

$$\mathbb{V}\mathrm{ar}\, g_{\mathcal{T}}(\boldsymbol{x}) \simeq \frac{\ell^* \, \boldsymbol{x}^\top \mathbf{H}_p^{-1} \boldsymbol{x}}{n} + \frac{\boldsymbol{x}^\top \mathbf{H}_p^{-1} \mathbf{M}_p \mathbf{H}_p^{-1} \boldsymbol{x}}{n}, \quad n \to \infty. \tag{2.55}$$

Figure 2.18 shows this (large-sample) variance of the learner for different values of the predictor u and model index p. Observe that the variance ultimately increases in p and that it is smaller at $u = 1/2$ than closer to the endpoints $u = 0$ or $u = 1$. Since the bias is also

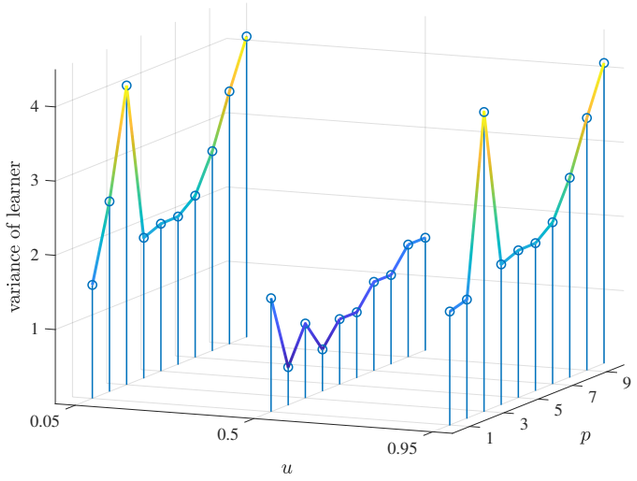


Figure 2.18: The pointwise variance of the learner for various pairs of p and u.

larger near the endpoints, we deduce that the pointwise mean squared error (2.21) is larger near the endpoints of the interval $[0, 1]$ than near its middle. In other words, the error is much smaller in the center of the data cloud than near its periphery.

☞ 405

JENSEN'S INEQUALITY

14. Let $h : \boldsymbol{x} \mapsto \mathbb{R}$ be a convex function and let $\boldsymbol{X}$ be a random variable. Use the subgradient definition of convexity to prove *Jensen's inequality*:

$$\mathbb{E}\, h(\boldsymbol{X}) \geqslant h(\mathbb{E}\boldsymbol{X}). \tag{2.56}$$

15. Using Jensen's inequality, show that the Kullback–Leibler divergence between probability densities f and g is always positive; that is,

$$\mathbb{E} \ln \frac{f(\boldsymbol{X})}{g(\boldsymbol{X})} \geqslant 0,$$

where $\boldsymbol{X} \sim f$.

VAPNIK–CHERNOVENKIS BOUND

16. The purpose of this exercise is to prove the following *Vapnik–Chernovenkis bound*: for any *finite* class $\mathcal{G}$ (containing only a finite number $|\mathcal{G}|$ of possible functions) and a general *bounded* loss function, $l \leqslant \text{Loss} \leqslant u$, the expected statistical error is bounded from above according to:

$$\mathbb{E}\, \ell(g^{\mathcal{G}}_{\mathcal{T}_n}) - \ell(g^{\mathcal{G}}) \leqslant \frac{(u-l)\sqrt{2\ln(2|\mathcal{G}|)}}{\sqrt{n}}. \tag{2.57}$$

Note how this bound conveniently does not depend on the distribution of the training set $\mathcal{T}_n$ (which is typically unknown), but only on the complexity (i.e., cardinality) of the class $\mathcal{G}$. We can break up the proof of (2.57) into the following four parts:

(a) For a general function class $\mathcal{G}$, training set $\mathcal{T}$, risk function ℓ, and training loss $\ell_{\mathcal{T}}$, we have, by definition, $\ell(g^{\mathcal{G}}) \leqslant \ell(g)$ and $\ell_{\mathcal{T}}(g^{\mathcal{G}}_{\mathcal{T}}) \leqslant \ell_{\mathcal{T}}(g)$ for all $g \in \mathcal{G}$. Show that

$$\ell(g^{\mathcal{G}}_{\mathcal{T}}) - \ell(g^{\mathcal{G}}) \leqslant \sup_{g\in\mathcal{G}} |\ell_{\mathcal{T}}(g) - \ell(g)| + \ell_{\mathcal{T}}(g^{\mathcal{G}}) - \ell(g^{\mathcal{G}}),$$

where we used the notation sup (supremum) for the least upper bound. Since $\mathbb{E}\ell_{\mathcal{T}}(g) = \mathbb{E}\ell(g)$, we obtain, after taking expectations on both sides of the inequality above:

$$\mathbb{E}\, \ell(g^{\mathcal{G}}_{\mathcal{T}}) - \ell(g^{\mathcal{G}}) \leqslant \mathbb{E} \sup_{g\in\mathcal{G}} |\ell_{\mathcal{T}}(g) - \ell(g)|.$$

HOEFFDING'S INEQUALITY

(b) If X is a zero-mean random variable taking values in the interval $[l, u]$, then the following *Hoeffding's inequality* states that the moment generating function satisfies

$$\mathbb{E}\, \mathrm{e}^{tX} \leqslant \exp\left(\frac{t^2(u-l)^2}{8}\right), \quad t \in \mathbb{R}. \tag{2.58}$$

Prove this result by using the fact that the line segment joining points $(l, \exp(tl))$ and $(u, \exp(tu))$ bounds the convex function $x \mapsto \exp(tx)$ for $x \in [l, u]$; that is:

$$\mathrm{e}^{tx} \leqslant \mathrm{e}^{tl}\frac{u-x}{u-l} + \mathrm{e}^{tu}\frac{x-l}{u-l}, \quad x \in [l, u].$$

(c) Let $Z_1, \ldots, Z_n$ be (possibly dependent and non-identically distributed) zero-mean random variables with moment generating functions that satisfy $\mathbb{E}\exp(tZ_k) \leqslant \exp(t^2\eta^2/2)$ for all k and some parameter η. Use Jensen's inequality (2.56) to prove that for any

☞ 429

$t > 0$,

$$\mathbb{E} \max_k Z_k = \frac{1}{t} \mathbb{E} \ln \max_k \mathrm{e}^{tZ_k} \leqslant \frac{1}{t} \ln n + \frac{t\eta^2}{2}.$$

From this derive that

$$\mathbb{E} \max_k Z_k \leqslant \eta \sqrt{2 \ln n}.$$

Finally, show that this last inequality implies that

$$\mathbb{E} \max_k |Z_k| \leqslant \eta \sqrt{2 \ln(2n)}. \tag{2.59}$$

(d) Returning to the objective of this exercise, denote the elements of $\mathcal{G}$ by $g_1, \ldots, g_{|\mathcal{G}|}$, and let $Z_k = \ell_{\mathcal{T}_n}(g_k) - \ell(g_k)$. By part (a) it is sufficient to bound $\mathbb{E} \max_k |Z_k|$. Show that the $\{Z_k\}$ satisfy the conditions of (c) with $\eta = (u - l)/\sqrt{n}$. For this you will need to apply part (b) to the random variable $\mathrm{Loss}(g(\boldsymbol{X}), Y) - \ell(g)$, where $(\boldsymbol{X}, Y)$ is a generic data point. Now complete the proof of (2.57).

17. Consider the problem in Exercise 16a above. Show that

$$|\ell_{\mathcal{T}}(g_{\mathcal{T}}^{\mathcal{G}}) - \ell(g^{\mathcal{G}})| \leqslant 2 \sup_{g \in \mathcal{G}} |\ell_{\mathcal{T}}(g) - \ell(g)| + \ell_{\mathcal{T}}(g^{\mathcal{G}}) - \ell(g^{\mathcal{G}}).$$

From this, conclude:

$$\mathbb{E} \, |\ell_{\mathcal{T}}(g_{\mathcal{T}}^{\mathcal{G}}) - \ell(g^{\mathcal{G}})| \leqslant 2 \mathbb{E} \sup_{g \in \mathcal{G}} |\ell_{\mathcal{T}}(g) - \ell(g)|.$$

The last bound allows us to assess how close the training loss $\ell_{\mathcal{T}}(g_{\mathcal{T}}^{\mathcal{G}})$ is to the optimal risk $\ell(g^{\mathcal{G}})$ within class $\mathcal{G}$.

18. Show that for the normal linear model $\boldsymbol{Y} \sim \mathcal{N}(\mathbf{X}\boldsymbol{\beta}, \sigma^2 \mathbf{I}_n)$, the maximum likelihood estimator of σ^2 is identical to the method of moments estimator (2.37).

19. Let $X \sim \mathsf{Gamma}(\alpha, \lambda)$. Show that the pdf of $Z = 1/X$ is equal to

$$\frac{\lambda^\alpha (z)^{-\alpha-1} \mathrm{e}^{-\lambda (z)^{-1}}}{\Gamma(\alpha)}, \quad z > 0.$$

20. Consider the sequence $w_0, w_1, \ldots$, where $w_0 = g(\boldsymbol{\theta})$ is a non-degenerate initial guess and $w_t(\boldsymbol{\theta}) \propto w_{t-1}(\boldsymbol{\theta}) g(\tau \,|\, \boldsymbol{\theta})$, $t > 1$. We assume that $g(\tau \,|\, \boldsymbol{\theta})$ is not the constant function (with respect to $\boldsymbol{\theta}$) and that the maximum likelihood value

$$g(\tau \,|\, \widehat{\boldsymbol{\theta}}) = \max_{\boldsymbol{\theta}} g(\tau \,|\, \boldsymbol{\theta}) < \infty$$

exists (is bounded). Let

$$l_t := \int g(\tau \,|\, \boldsymbol{\theta}) w_t(\boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{\theta}.$$

Show that $\{l_t\}$ is a strictly increasing and bounded sequence. Hence, conclude that its limit is $g(\tau \,|\, \widehat{\boldsymbol{\theta}})$.

21. Consider the Bayesian model for $\tau = \{x_1, \ldots, x_n\}$ with likelihood $g(\tau \,|\, \mu)$ such that $(X_1, \ldots, X_n \,|\, \mu) \sim_{\text{iid}} \mathcal{N}(\mu, 1)$ and prior pdf $g(\mu)$ such that $\mu \sim \mathcal{N}(\nu, 1)$ for some hyperparameter ν. Define a sequence of densities $w_t(\mu), t \geqslant 2$ via $w_t(\mu) \propto w_{t-1}(\mu)\, g(\tau \,|\, \mu)$, starting with $w_1(\mu) = g(\mu)$. Let a_t and b_t denote the mean and precision[4] of μ under the posterior $g_t(\mu \,|\, \tau) \propto g(\tau \,|\, \mu) w_t(\mu)$. Show that $g_t(\mu \,|\, \tau)$ is a normal density with precision $b_t = b_{t-1} + n,\ b_0 = 1$ and mean $a_t = (1 - \gamma_t) a_{t-1} + \gamma_t \overline{x}_n,\ a_0 = \nu$, where $\gamma_t := n/(b_{t-1} + n)$. Hence, deduce that $g_t(\mu \,|\, \tau)$ converges to a degenerate density with a point-mass at $\overline{x}_n$.

22. Consider again Example 2.8, where we have a normal model with improper prior $g(\boldsymbol{\theta}) = g(\mu, \sigma^2) \propto 1/\sigma^2$. Show that the prior predictive pdf is an improper density $g(x) \propto 1$, but that the posterior predictive density is

$$g(x \,|\, \tau) \propto \left(1 + \frac{(x - \overline{x}_n)^2}{(n+1) S_n^2}\right)^{-n/2}.$$

Deduce that $\frac{X - \overline{x}_n}{S_n \sqrt{(n+1)/(n-1)}} \sim \mathsf{t}_{n-1}$.

23. Assuming that $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n \overset{\text{iid}}{\sim} f$, show that (2.48) holds and that $\ell_n^* = -n\, \mathbb{E} \ln f(\boldsymbol{X})$.

24. Suppose that $\tau = \{x_1, \ldots, x_n\}$ are observations of iid continuous and strictly positive random variables, and that there are two possible models for their pdf. The first model $p = 1$ is

$$g(x \,|\, \theta, p = 1) = \theta \exp(-\theta x)$$

and the second $p = 2$ is

$$g(x \,|\, \theta, p = 2) = \left(\frac{2\theta}{\pi}\right)^{1/2} \exp\left(-\frac{\theta x^2}{2}\right).$$

For both models, assume that the prior for θ is a gamma density

$$g(\theta) = \frac{b^t}{\Gamma(t)} \theta^{t-1} \exp(-b\theta),$$

with the same hyperparameters b and t. Find a formula for the Bayes factor, $g(\tau \,|\, p = 1)/g(\tau \,|\, p = 2)$, for comparing these models.

25. Suppose that we have a total of m possible models with prior probabilities $g(p), p = 1, \ldots, m$. Show that the posterior probability of model $g(p \,|\, \tau)$ can be expressed in terms of all the $p(p-1)$ Bayes factors:

$$g(p = i \,|\, \tau) = \left(1 + \sum_{j \neq i} \frac{g(p = j)}{g(p = i)} B_{j|i}\right)^{-1}.$$

[4] The precision is the reciprocal of the variance.

26. Given the data $\tau = \{x_1, \ldots, x_n\}$, suppose that we use the likelihood $(X \,|\, \boldsymbol{\theta}) \sim \mathcal{N}(\mu, \sigma^2)$ with parameter $\boldsymbol{\theta} = (\mu, \sigma^2)^\top$ and wish to compare the following two nested models.

(a) Model $p = 1$, where $\sigma^2 = \sigma_0^2$ is known and this is incorporated via the prior

$$g(\boldsymbol{\theta} \,|\, p = 1) = g(\mu \,|\, \sigma^2, p = 1)\, g(\sigma^2 \,|\, p = 1) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(\mu - x_0)^2}{2\sigma^2}} \times \delta(\sigma^2 - \sigma_0^2).$$

(b) Model $p = 2$, where both mean and variance are unknown with prior

$$g(\boldsymbol{\theta} \,|\, p = 2) = g(\mu \,|\, \sigma^2)\, g(\sigma^2) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(\mu - x_0)^2}{2\sigma^2}} \times \frac{b^t (\sigma^2)^{-t-1} \mathrm{e}^{-b/\sigma^2}}{\Gamma(t)}.$$

Show that the prior $g(\boldsymbol{\theta} \,|\, p = 1)$ can be viewed as the limit of the prior $g(\boldsymbol{\theta} \,|\, p = 2)$ when $t \to \infty$ and $b = t\sigma_0^2$. Hence, conclude that

$$g(\tau \,|\, p = 1) = \lim_{\substack{t \to \infty \\ b = t\sigma_0^2}} g(\tau \,|\, p = 2)$$

and use this result to calculate $B_{1\,|\,2}$. Check that the formula for $B_{1\,|\,2}$ agrees with the Savage–Dickey density ratio:

$$\frac{g(\tau \,|\, p = 1)}{g(\tau \,|\, p = 2)} = \frac{g(\sigma^2 = \sigma_0^2 \,|\, \tau)}{g(\sigma^2 = \sigma_0^2)},$$

where $g(\sigma^2 \,|\, \tau)$ and $g(\sigma^2)$ are the posterior and prior, respectively, under model $p = 2$.

CHAPTER 3

MONTE CARLO METHODS

Many algorithms in machine learning and data science make use of Monte Carlo techniques. This chapter gives an introduction to the three main uses of Monte Carlo simulation: to (1) simulate random objects and processes in order to observe their behavior, (2) estimate numerical quantities by repeated sampling, and (3) solve complicated optimization problems through randomized algorithms.

3.1 Introduction

MONTE CARLO SIMULATION

Briefly put, *Monte Carlo simulation* is the generation of random data by means of a computer. These data could arise from simple models, such as those described in Chapter 2, or from very complicated models describing real-life systems, such as the positions of vehicles on a complex road network, or the evolution of security prices in the stock market. In many cases, Monte Carlo simulation simply involves random sampling from certain probability distributions. The idea is to repeat the random experiment that is described by the model many times to obtain a large quantity of data that can be used to answer questions about the model. The three main uses of Monte Carlo simulation are:

Sampling. Here the objective is to gather information about a random object by observing many realizations of it. For instance, this could be a random process that mimics the behavior of some real-life system such as a production line or telecommunications network. Another usage is found in Bayesian statistics, where Markov chains are often used to sample from a posterior distribution. ☞ 48

Estimation. In this case the emphasis is on estimating certain numerical quantities related to a simulation model. An example is the evaluation of multidimensional integrals via Monte Carlo techniques. This is achieved by writing the integral as the expectation of a random variable, which is then approximated by the sample mean. Appealing to the Law of Large Numbers guarantees that this approximation will eventually converge when the sample size becomes large. ☞ 448

Optimization. Monte Carlo simulation is a powerful tool for the optimization of complicated objective functions. In many applications these functions are deterministic and

randomness is introduced artificially in order to more efficiently search the domain of the objective function. Monte Carlo techniques are also used to optimize noisy functions, where the function itself is random; for example, when the objective function is the output of a Monte Carlo simulation.

The Monte Carlo method dramatically changed the way in which statistics is used in today's analysis of data. The ever-increasing complexity of data requires radically different statistical models and analysis techniques from those that were used 20 to 100 years ago. By using Monte Carlo techniques, the data analyst is no longer restricted to using basic (and often inappropriate) models to describe data. Now, any probabilistic model that can be simulated on a computer can serve as the basis for statistical analysis. This Monte Carlo revolution has had an impact on both Bayesian and frequentist statistics. In particular, in frequentist statistics, Monte Carlo methods are often referred to as resampling techniques. An important example is the well-known bootstrap method [37], where statistical quantities such as confidence intervals and P-values for statistical tests can simply be determined by simulation without the need of a sophisticated analysis of the underlying probability distributions; see, for example, [69] for basic applications. The impact on Bayesian statistics has been even more profound, through the use of Markov chain Monte Carlo (MCMC) techniques [87, 48]. MCMC samplers construct a Markov process which converges in distribution to a desired (often high-dimensional) density. This convergence in distribution justifies using a finite run of the Markov process as an approximate random realization from the target density. The MCMC approach has rapidly gained popularity as a versatile heuristic approximation, partly due to its simple computer implementation and inbuilt mechanism to tradeoff between computational cost and accuracy; namely, the longer one runs the Markov process, the better the approximation. Nowadays, MCMC methods are indispensable for analyzing posterior distributions for inference and model selection; see also [50, 99].

The following three sections elaborate on these three uses of Monte Carlo simulation in turn.

3.2 Monte Carlo Sampling

In this section we describe a variety of Monte Carlo sampling methods, from the building block of simulating uniform random numbers to MCMC samplers.

3.2.1 Generating Random Numbers

RANDOM NUMBER GENERATOR

At the heart of any Monte Carlo method is a *random number generator*: a procedure that produces a stream of uniform random numbers on the interval (0,1). Since such numbers are usually produced via deterministic algorithms, they are not truly random. However, for most applications all that is required is that such pseudo-random numbers are statistically indistinguishable from genuine random numbers $U_1, U_2, \ldots$ that are uniformly distributed on the interval (0,1) and are independent of each other; we write $U_1, U_2, \ldots \sim_{\text{iid}} \mathcal{U}(0,1)$. For example, in Python the `rand` method of the `numpy.random` module is widely used for this purpose.

Most random number generators at present are based on linear recurrence relations. One of the most important random number generators is the *multiple-recursive generator* (MRG) of *order* k, which generates a sequence of integers $X_k, X_{k+1}, \ldots$ via the linear recurrence

MULTIPLE-RECURSIVE GENERATOR

$$X_t = (a_1 X_{t-1} + \cdots + a_k X_{t-k}) \bmod m, \quad t = k, k+1, \ldots \tag{3.1}$$

for some *modulus* m and *multipliers* $\{a_i, i = 1, \ldots, k\}$. Here "mod" refers to the modulo operation: $n \bmod m$ is the remainder when n is divided by m. The recurrence is initialized by specifying k "seeds", $X_0, \ldots, X_{k-1}$. To yield fast algorithms, all but a few of the multipliers should be 0. When m is a large integer, one can obtain a stream of pseudo-random numbers $U_k, U_{k+1}, \ldots$ between 0 and 1 from the sequence $X_k, X_{k+1}, \ldots$, simply by setting $U_t = X_t/m$. It is also possible to set a small modulus, in particular $m = 2$. The output function for such *modulo 2 generators* is then typically of the form

MODULUS
MULTIPLIERS

MODULO 2 GENERATORS

$$U_t = \sum_{i=1}^{w} X_{tw+i-1} 2^{-i}$$

for some $w \leqslant k$, e.g., $w = 32$ or 64. Examples of modulo 2 generators are the *feedback shift register* generators, the most popular of which are the *Mersenne twisters*; see, for example, [79] and [83]. MRGs with excellent statistical properties can be implemented efficiently by combining several simpler MRGs and carefully choosing their respective moduli and multipliers. One of the most successful is L'Ecuyer's `MRG32k3a` generator; see [77]. From now on, we assume that the reader has a sound random number generator available.

FEEDBACK SHIFT REGISTER

MERSENNE TWISTERS

3.2.2 Simulating Random Variables

Simulating a random variable X from an arbitrary (that is, not necessarily uniform) distribution invariably involves the following two steps:

1. Simulate uniform random numbers $U_1, \ldots, U_k$ on $(0, 1)$ for some $k = 1, 2, \ldots$.
2. Return $X = g(U_1, \ldots, U_k)$, where g is some real-valued function.

The construction of suitable functions g is as much of an art as a science. Many simulation methods may be found, for example, in [71] and the accompanying website `www.montecarlohandbook.org`. Two of the most useful general procedures for generating random variables are the *inverse-transform* method and the *acceptance–rejection* method. Before we discuss these, we show one possible way to simulate standard normal random variables. In Python we can generate standard normal random variables via the `randn` method of the `numpy.random` module.

■ **Example 3.1 (Simulating Standard Normal Random Variables)** If X and Y are independent standard normally distributed random variables (that is, $X, Y \sim_{\text{iid}} \mathcal{N}(0, 1)$), then their joint pdf is

$$f(x, y) = \frac{1}{2\pi} \mathrm{e}^{-\frac{1}{2}(x^2+y^2)}, \quad (x, y) \in \mathbb{R}^2,$$

which is a radially symmetric function. In Example C.2 we see that, in polar coordinates, the angle Θ that the random vector $[X, Y]^\top$ makes with the positive x-axis is $\mathcal{U}(0, 2\pi)$

☞ 435

distributed (as would be expected from the radial symmetry) and the radius R has pdf $f_R(r) = r\,\mathrm{e}^{-r^2/2}, r > 0$. Moreover, R and Θ are independent. We will see shortly, in Example 3.4, that R has the same distribution as $\sqrt{-2\ln U}$ with $U \sim \mathcal{U}(0,1)$. So, to simulate $X, Y \sim_{\text{iid}} \mathcal{N}(0,1)$, the idea is to first simulate R and Θ independently and then return $X = R\cos(\Theta)$ and $Y = R\sin(\Theta)$ as a pair of independent standard normal random variables. This leads to the Box–Muller approach for generating standard normal random variables.

☞ 72

Algorithm 3.2.1: Normal Random Variable Simulation: Box–Muller Approach

output: Independent standard normal random variables X and Y.
1 Simulate two independent random variables, U_1 and U_2, from $\mathcal{U}(0,1)$.
2 $X \leftarrow (-2\ln U_1)^{1/2}\cos(2\pi U_2)$
3 $Y \leftarrow (-2\ln U_1)^{1/2}\sin(2\pi U_2)$
4 **return** X, Y

■

Once a standard normal number generator is available, simulation from any n-dimensional normal distribution $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ is relatively straightforward. The first step is to find an $n \times n$ matrix $\mathbf{B}$ that decomposes $\boldsymbol{\Sigma}$ into the matrix product $\mathbf{B}\mathbf{B}^\top$. In fact there exist many such decompositions. One of the more important ones is the *Cholesky decomposition*, which is a special case of the LU decomposition; see Section A.6.1 for more information on such decompositions. In Python, the function `cholesky` of `numpy.linalg` can be used to produce such a matrix $\mathbf{B}$.

CHOLESKY DECOMPOSITION

☞ 370

Once the Cholesky factorization is determined, it is easy to simulate $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ as, by definition, it is the affine transformation $\boldsymbol{\mu} + \mathbf{B}\boldsymbol{Z}$ of an n-dimensional standard normal random vector.

Algorithm 3.2.2: Normal Random Vector Simulation

input: $\boldsymbol{\mu}, \boldsymbol{\Sigma}$
output: $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$
1 Determine the Cholesky factorization $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$.
2 Simulate $\boldsymbol{Z} = [Z_1, \ldots, Z_n]^\top$ by drawing $Z_1, \ldots, Z_n \sim_{\text{iid}} \mathcal{N}(0,1)$.
3 $\boldsymbol{X} \leftarrow \boldsymbol{\mu} + \mathbf{B}\boldsymbol{Z}$
4 **return** $\boldsymbol{X}$

■ **Example 3.2 (Simulating from a Bivariate Normal Distribution)** The Python code below draws $N = 1000$ iid samples from the two bivariate ($n = 2$) normal pdfs in Figure 2.13. The resulting point clouds are given in Figure 3.1.

☞ 45

bvnormal.py

```
import numpy as np
from numpy.random import randn
import matplotlib.pyplot as plt

N = 1000
r = 0.0   #change to 0.8 for other plot
Sigma = np.array([[1, r], [r, 1]])
```

```
B = np.linalg.cholesky(Sigma)
x = B @ randn(2,N)
plt.scatter([x[0,:]],[x[1,:]], alpha =0.4, s = 4)
```

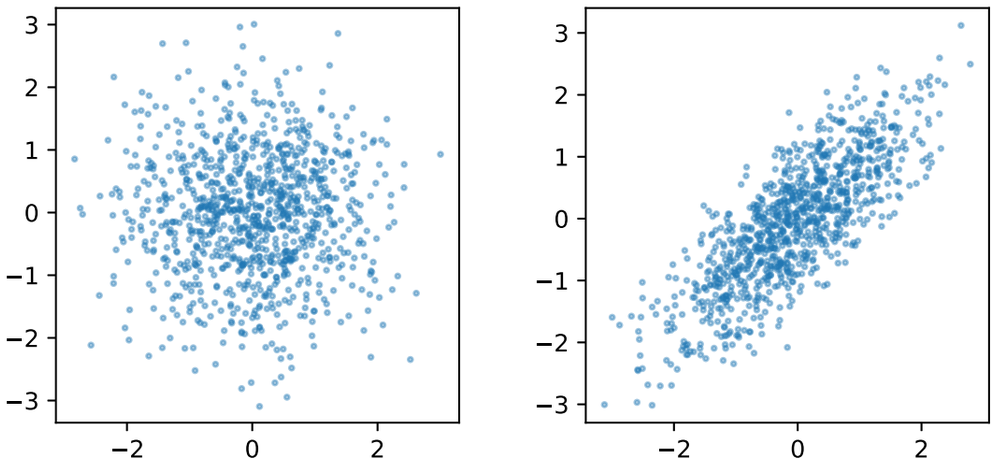


Figure 3.1: 1000 realizations of bivariate normal distributions with means zero, variances 1, and correlation coefficients 0 (left) and 0.8 (right).

■

In some cases, the covariance matrix $\boldsymbol{\Sigma}$ has special structure which can be exploited to create even faster generation algorithms, as illustrated in the following example.

■ **Example 3.3 (Simulating Normal Vectors in $O(n^2)$ Time)** Suppose that the random vector $\boldsymbol{X} = [X_1, \ldots, X_n]^\top$ represents the values at times $t_0 + k\delta$, $k = 0, \ldots, n-1$ of a zero-mean *Gaussian process* $(X(t), t \geqslant 0)$ that is *weakly stationary*, meaning that $\mathbb{C}\mathrm{ov}(X(s), X(t))$ depends only on $t-s$. Then clearly the covariance matrix of $\boldsymbol{X}$, say $\mathbf{A}_n$, is a symmetric Toeplitz matrix. Suppose for simplicity that $\mathbb{V}\mathrm{ar}\, X(t) = 1$. Then the covariance matrix is in fact a correlation matrix, and will have the following structure:

☞ 239
☞ 381

$$\mathbf{A}_n := \begin{bmatrix} 1 & a_1 & \ldots & a_{n-2} & a_{n-1} \\ a_1 & 1 & \ddots & & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{n-2} & & \ddots & \ddots & a_1 \\ a_{n-1} & a_{n-2} & \cdots & a_1 & 1 \end{bmatrix}.$$

Using the Levinson–Durbin algorithm we can compute a lower diagonal matrix $\mathbf{L}_n$ and a diagonal matrix $\mathbf{D}_n$ in $O(n^2)$ time such that $\mathbf{L}_n \mathbf{A}_n \mathbf{L}_n^\top = \mathbf{D}_n$; see Theorem A.14. If we simulate $\boldsymbol{Z}_n \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$, then the solution $\boldsymbol{X}$ of the linear system:

☞ 385

$$\mathbf{L}_n \boldsymbol{X} = \mathbf{D}_n^{1/2} \boldsymbol{Z}_n$$

has the desired distribution $\mathcal{N}(\mathbf{0}, \mathbf{A}_n)$. The linear system is solved in $O(n^2)$ time via forward substitution. ■

3.2.2.1 Inverse-Transform Method

Let X be a random variable with cumulative distribution function (cdf) F. Let F^{-1} denote the inverse[1] of F and $U \sim \mathcal{U}(0,1)$. Then,

$$\mathbb{P}[F^{-1}(U) \leqslant x] = \mathbb{P}[U \leqslant F(x)] = F(x). \tag{3.2}$$

This leads to the following method to simulate a random variable X with cdf F:

Algorithm 3.2.3: Inverse-Transform Method

input: Cumulative distribution function F.
output: Random variable X distributed according to F.

1 Generate U from $\mathcal{U}(0,1)$.
2 $X \leftarrow F^{-1}(U)$
3 **return** X

The inverse-transform method works both for continuous and discrete distributions. After importing `numpy` as `np`, simulating numbers $0, \ldots, k-1$ according to probabilities $p_0, \ldots, p_{k-1}$ can be done via `np.min(np.where(np.cumsum(p) > np.random.rand()))`, where `p` is the vector of the probabilities.

■ **Example 3.4 (Example 3.1 (cont.))** One remaining issue in Example 3.1 was how to simulate the radius R when we only know its density $f_R(r) = r\,\mathrm{e}^{-r^2/2}$, $r > 0$. We can use the inverse-transform method for this, but first we need to determine its cdf. The cdf of R is, by integration of the pdf,

$$F_R(r) = 1 - \mathrm{e}^{-\frac{1}{2}r^2}, \quad r > 0,$$

and its inverse is found by solving $u = F_R(r)$ in terms of r, giving

$$F_R^{-1}(u) = \sqrt{-2\ln(1-u)}, \quad u \in (0,1).$$

Thus R has the same distribution as $\sqrt{-2\ln(1-U)}$, with $U \sim \mathcal{U}(0,1)$. Since $1-U$ also has a $\mathcal{U}(0,1)$ distribution, R has also the same distribution as $\sqrt{-2\ln U}$. ■

3.2.2.2 Acceptance–Rejection Method

The acceptance–rejection method is used to sample from a "difficult" probability density function (pdf) $f(x)$ by generating instead from an "easy" pdf $g(x)$ satisfying $f(x) \leqslant C\,g(x)$ for some constant $C \geqslant 1$ (for example, via the inverse-transform method), and then accepting or rejecting the drawn sample with a certain probability. Algorithm 3.2.4 gives the pseudo-code.

The idea of the algorithm is to generate uniformly a point (X, Y) under the graph of the function Cg, by first drawing $X \sim g$ and then $Y \sim \mathcal{U}(0, Cg(X))$. If this point lies under the graph of f, then we accept X as a sample from f; otherwise, we try again. The efficiency of the acceptance–rejection method is usually expressed in terms of the probability of acceptance, which is $1/C$.

[1] Every cdf has a unique inverse function defined by $F^{-1}(u) = \inf\{x : F(x) \geqslant u\}$. If, for each u, the equation $F(x) = u$ has a unique solution x, this definition coincides with the usual interpretation of the inverse function.

Algorithm 3.2.4: Acceptance–Rejection Method

input: Pdf g and constant C such that $Cg(x) \geqslant f(x)$ for all x.
output: Random variable X distributed according to pdf f.

found $\leftarrow$ **false**
while not found **do**
  Generate X from g.
  Generate U from $\mathcal{U}(0,1)$ independently of X.
  $Y \leftarrow UCg(X)$
  if $Y \leqslant f(X)$ **then** found $\leftarrow$ **true**
return X

■ **Example 3.5 (Simulating Gamma Random Variables)** Simulating random variables from a Gamma(α, λ) distribution is generally done via the acceptance–rejection method. Consider, for example, the Gamma distribution with $\alpha = 1.3$ and $\lambda = 5.6$. Its pdf, ☞ 427

$$f(x) = \frac{\lambda^\alpha x^{\alpha-1} \mathrm{e}^{-\lambda x}}{\Gamma(\alpha)}, \quad x \geqslant 0,$$

where Γ is the gamma function $\Gamma(\alpha) := \int_0^\infty \mathrm{e}^{-x} x^{\alpha-1}\,\mathrm{d}x$, $\alpha > 0$, is depicted by the blue solid curve in Figure 3.2.

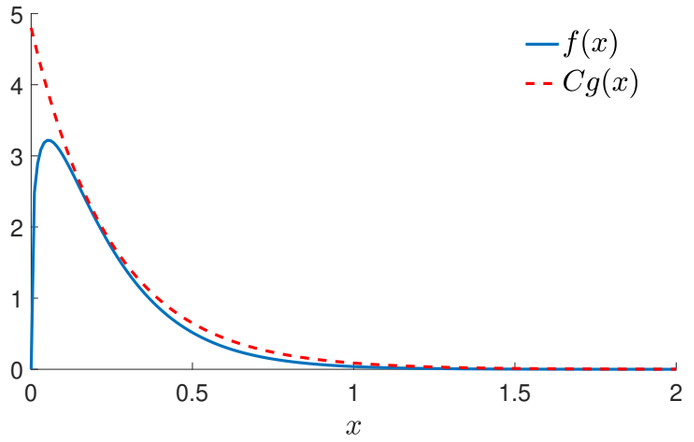


Figure 3.2: The pdf g of the Exp(4) distribution multiplied by $C = 1.2$ dominates the pdf f of the Gamma(1.3, 5.6) distribution.

This pdf happens to lie completely under the graph of $Cg(x)$, where $C = 1.2$ and $g(x) = 4\exp(-4x), x \geqslant 0$ is the pdf of the exponential distribution Exp(4). Hence, we can simulate from this particular Gamma distribution by accepting or rejecting a sample from the Exp(4) distribution according to Step 6 of Algorithm 3.2.4. Simulating from the Exp(4) distribution can be done via the inverse-transform method: simulate $U \sim \mathcal{U}(0,1)$ and return $X = -\ln(U)/4$. The following Python code implements Algorithm 3.2.4 for this example. ☞ 427

accrejgamma.py

```
from math import exp, gamma, log
from numpy.random import rand

alpha = 1.3
lam = 5.6
f = lambda x: lam**alpha * x**(alpha-1) * exp(-lam*x)/gamma(alpha)
g = lambda x: 4*exp(-4*x)
C = 1.2

found = False
while not found:
    x = - log(rand())/4
    if C*g(x)*rand() <= f(x):
        found = True

print(x)
```

■

3.2.3 Simulating Random Vectors and Processes

Techniques for generating random vectors and processes are as diverse as the class of random processes themselves; see, for example, [71]. We highlight a few general scenarios.

When $X_1, \ldots, X_n$ are *independent* random variables with pdfs f_i, $i = 1, \ldots, n$, so that
☞ 431
their joint pdf is $f(\boldsymbol{x}) = f_1(x_1) \cdots f_n(x_n)$, the random vector $\boldsymbol{X} = [X_1, \ldots, X_n]^\top$ can be simply simulated by drawing each component $X_i \sim f_i$ individually — for example, via the inverse-transform method or acceptance–rejection.

For *dependent* components $X_1, \ldots, X_n$, we can, as a consequence of the *product rule* of
☞ 433
probability, represent the joint pdf $f(\boldsymbol{x})$ as

$$f(\boldsymbol{x}) = f(x_1, \ldots, x_n) = f_1(x_1)\, f_2(x_2 \,|\, x_1) \cdots f_n(x_n \,|\, x_1, \ldots, x_{n-1}), \tag{3.3}$$

where $f_1(x_1)$ is the marginal pdf of X_1 and $f_k(x_k \,|\, x_1, \ldots, x_{k-1})$ is the conditional pdf of X_k given $X_1 = x_1, X_2 = x_2, \ldots, X_{k-1} = x_{k-1}$. Provided the conditional pdfs are known, one can generate $\boldsymbol{X}$ by first generating X_1, then, given $X_1 = x_1$, generate X_2 from $f_2(x_2 \,|\, x_1)$, and so on, until generating X_n from $f_n(x_n \,|\, x_1, \ldots, x_{n-1})$.

The latter method is particularly applicable for generating Markov chains. Recall from
☞ 453
Section C.10 that a *Markov chain* is a stochastic process $\{X_t, t = 0, 1, 2, \ldots\}$ that satisfies
MARKOV CHAIN
the *Markov property*; meaning that for all t and s the conditional distribution of X_{t+s} given $X_u, u \leqslant t$, is the same as that of X_{t+s} given only X_t. As a result, each conditional density $f_t(x_t \,|\, x_1, \ldots, x_{t-1})$ can be written as a one-step *transition density* $q_t(x_t \,|\, x_{t-1})$; that is, the probability density to go from state x_{t-1} to state x_t in one step. In many cases of interest the chain is *time-homogeneous*, meaning that the transition density q_t does not depend on t. Such Markov chains can be generated *sequentially*, as given in Algorithm 3.2.5.

Algorithm 3.2.5: Simulate a Markov Chain

input: Number of steps N, initial pdf f_0, transition density q.

1 Draw X_0 from the initial pdf f_0.
2 **for** $t = 1$ **to** N **do**
3 Draw X_t from the distribution corresponding to the density $q(\cdot \,|\, X_{t-1})$
4 **return** $X_0, \ldots, X_N$

■ **Example 3.6 (Markov Chain Simulation)** For time-homogeneous Markov chains with a discrete state space, we can visualize the one-step transitions by means of a *transition graph*, where arrows indicate possible transitions between states and the labels describe the corresponding probabilities. Figure 3.3 shows (on the left) the transition graph of the Markov chain $\{X_t, t = 0, 1, 2, \ldots\}$ with state space $\{1, 2, 3, 4\}$ and one-step transition matrix

TRANSITION GRAPH

$$\mathbf{P} = \begin{bmatrix} 0 & 0.2 & 0.5 & 0.3 \\ 0.5 & 0 & 0.5 & 0 \\ 0.3 & 0.7 & 0 & 0 \\ 0.1 & 0 & 0 & 0.9 \end{bmatrix}.$$

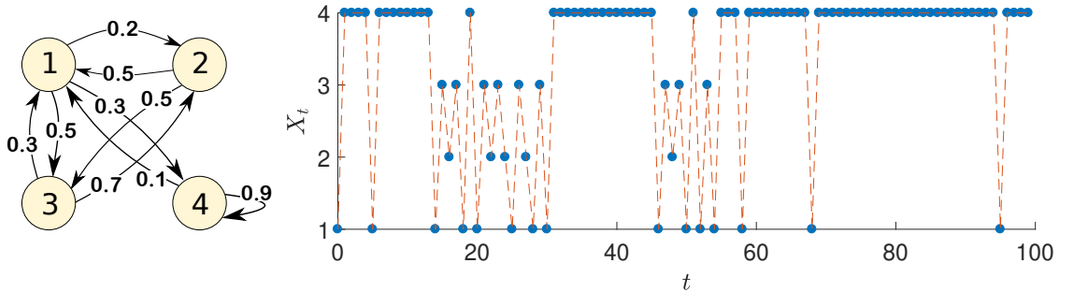


Figure 3.3: The transition graph (left) and a typical path (right) of the Markov chain.

In the same figure (on the right) a typical outcome (path) of the Markov chain is shown. The path was simulated using the Python program below. In this implementation the Markov chain always starts in state 1. We will revisit Markov chains, and in particular Markov chains with continuous state spaces, in Section 3.2.5.

☞ 78

MCsim.py

```
import numpy as np
import matplotlib.pyplot as plt

n = 101
P = np.array([[0, 0.2, 0.5, 0.3],
              [0.5, 0, 0.5, 0],
              [0.3, 0.7, 0, 0],
              [0.1, 0, 0, 0.9]])
x = np.array(np.ones(n, dtype=int))
x[0] = 0
for t in range(0,n-1):
```

```
    x[t+1] = np.min(np.where(np.cumsum(P[x[t],:]) >
                     np.random.rand()))
x = x + 1  #add 1 to all elements of the vector x
plt.plot(np.array(range(0,n)),x, 'o')
plt.plot(np.array(range(0,n)),x, '--')
plt.show()
```

■

3.2.4 Resampling

RESAMPLING

The idea behind *resampling* is very simple: an iid sample $\tau := \{x_1, \ldots, x_n\}$ from some unknown cdf F represents our best knowledge of F if we make no further *a priori* assumptions about it. If it is not possible to simulate more samples from F, the best way to "repeat" the experiment is to *resample* from the original data by drawing from the empirical cdf F_n; see (1.2). That is, we draw each x_i with equal probability and repeat this N times, according to Algorithm 3.2.6 below. As we draw here "with replacement", multiple instances of the original data points may occur in the resampled data.

☞ 11

Algorithm 3.2.6: Sampling from an Empirical Cdf.

input: Original iid sample $x_1, \ldots, x_n$ and sample size N.
output: Iid sample $X_1^*, \ldots, X_N^*$ from the empirical cdf.

1 **for** $t = 1$ **to** N **do**
2 Draw $U \sim \mathcal{U}(0, 1)$
3 Set $I \leftarrow \lceil nU \rceil$
4 Set $X_t^* \leftarrow x_I$
5 **return** $X_1^*, \ldots, X_N^*$

In Step 3, $\lceil nU \rceil$ returns the *ceiling* of nU; that is, it is the smallest integer larger than or equal to nU. Consequently, I is drawn uniformly at random from the set of indices $\{1, \ldots, n\}$.

By sampling from the empirical cdf we can thus (approximately) repeat the experiment that gave us the original data as many times as we like. This is useful if we want to assess the properties of certain statistics obtained from the data. For example, suppose that the original data τ gave the statistic $t(\tau)$. By resampling we can gain information about the *distribution* of the corresponding random variable $t(\mathcal{T})$.

■ **Example 3.7 (Quotient of Uniforms)** Let $U_1, \ldots, U_n, V_1, \ldots, V_n$ be iid $\mathcal{U}(0, 1)$ random variables and define $X_i = U_i/V_i$, $i = 1, \ldots, n$. Suppose we wish to investigate the distribution of the sample median $\widetilde{X}$ and sample mean $\overline{X}$ of the (random) data $\mathcal{T} := \{X_1, \ldots, X_n\}$. Since we know the model for $\mathcal{T}$ exactly, we can generate a large number, N say, of independent copies of it, and for each of these copies evaluate the sample medians $\widetilde{X}_1, \ldots, \widetilde{X}_N$ and sample means $\overline{X}_1, \ldots, \overline{X}_N$. For $n = 100$ and $N = 1000$ the empirical cdfs might look like the left and right curves in Figure 3.4, respectively. Contrary to what you might have expected, the distributions of the sample median and sample mean do not match at all. The sample median is quite concentrated around 1, whereas the distribution of the sample mean is much more spread out.

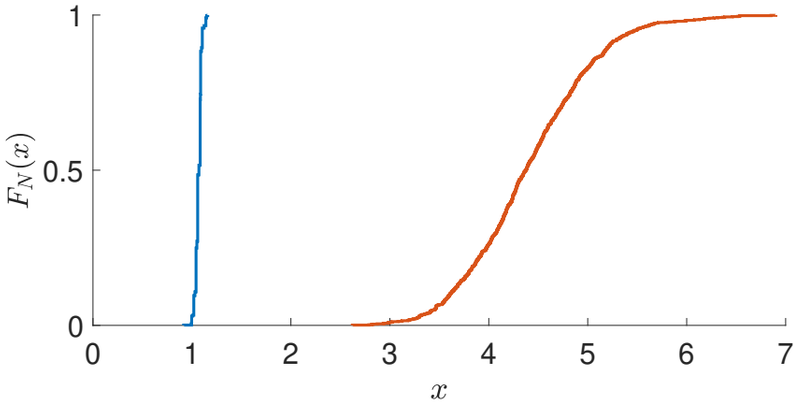


Figure 3.4: Empirical cdfs of the medians of the resampled data (left curve) and sample means (right curve) of the resampled data.

Instead of sampling completely new data, we could also *reuse* the original data by resampling them via Algorithm 3.2.6. This gives independent copies $\widetilde{X}_1^*, \ldots, \widetilde{X}_N^*$ and $\overline{X}_1^*, \ldots, \overline{X}_N^*$, for which we can again plot the empirical cdf. The results will be similar to the previous case. In fact, in Figure 3.4 the cdf of the *resampled* sample medians and sample means are plotted. The corresponding Python code is given below. The essential point of this example is that resampling of data can greatly add to the understanding of the probabilistic properties of certain measurements on the data, *even if the underlying model is not known*. See Exercise 12 for a further investigation of this example. ☞ 116

quotunif.py

```
import numpy as np
from numpy.random import rand, choice
import matplotlib.pyplot as plt
from statsmodels.distributions.empirical_distribution import ECDF

n = 100
N = 1000
x = rand(n)/rand(n)  # data
med = np.zeros(N)
ave = np.zeros(N)
for i in range(0,N):
    s = choice(x, n, replace=True) # resampled data
    med[i] = np.median(s)
    ave[i] = np.mean(s)

med_cdf = ECDF(med)
ave_cdf = ECDF(ave)
plt.plot(med_cdf.x, med_cdf.y)
plt.plot(ave_cdf.x, ave_cdf.y)
plt.show()
```

■

3.2.5 Markov Chain Monte Carlo

MARKOV CHAIN MONTE CARLO

TARGET

Markov chain Monte Carlo (MCMC) is a Monte Carlo sampling technique for (approximately) generating samples from an arbitrary distribution — often referred to as the *target* distribution. The basic idea is to run a Markov chain long enough such that its limiting distribution is close to the target distribution. Often such a Markov chain is constructed to be reversible, so that the detailed balance equations (C.43) can be used. Depending on the starting position of the Markov chain, the initial random variables in the Markov chain may have a distribution that is significantly different from the target (limiting) distribution. The random variables that are generated during this *burn-in period* are often discarded. The remaining random variables form an *approximate* and *dependent* sample from the target distribution.

☞ 455

BURN-IN PERIOD

In the next two sections we discuss two popular MCMC samplers: the Metropolis–Hastings sampler and the Gibbs sampler.

3.2.5.1 Metropolis–Hastings Sampler

☞ 72

The Metropolis–Hastings sampler [87] is similar to the acceptance–rejection method in that it simulates a trial state, which is then accepted or rejected according to some random mechanism. Specifically, suppose we wish to sample from a target pdf $f(\boldsymbol{x})$, where $\boldsymbol{x}$ takes values in some d-dimensional set. The aim is to construct a Markov chain $\{\boldsymbol{X}_t, t = 0, 1, \ldots\}$ in such a way that its limiting pdf is f. Suppose the Markov chain is in state $\boldsymbol{x}$ at time t. A transition of the Markov chain from state $\boldsymbol{x}$ is carried out in two phases. First a *proposal* state $\boldsymbol{Y}$ is drawn from a transition density $q(\cdot \,|\, \boldsymbol{x})$. This state is accepted as the new state, with *acceptance probability*

PROPOSAL

ACCEPTANCE PROBABILITY

$$\alpha(\boldsymbol{x}, \boldsymbol{y}) = \min\left\{\frac{f(\boldsymbol{y})\, q(\boldsymbol{x} \,|\, \boldsymbol{y})}{f(\boldsymbol{x})\, q(\boldsymbol{y} \,|\, \boldsymbol{x})}, 1\right\}, \tag{3.4}$$

or rejected otherwise. In the latter case the chain remains in state $\boldsymbol{x}$. The algorithm just described can be summarized as follows.

Algorithm 3.2.7: Metropolis–Hastings Sampler

input: Initial state $\boldsymbol{X}_0$, sample size N, target pdf $f(\boldsymbol{x})$, proposal function $q(\boldsymbol{y} \,|\, \boldsymbol{x})$.
output: $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$ (dependent), approximately distributed according to $f(\boldsymbol{x})$.

```
for t = 0 to N − 1 do
    Draw Y ∼ q(y | X_t)                          // draw a proposal
    α ← α(X_t, Y)                  // acceptance probability as in (3.4)
    Draw U ∼ U(0, 1)
    if U ⩽ α then X_{t+1} ← Y
    else X_{t+1} ← X_t
return X_1, ..., X_N
```

The fact that the limiting distribution of the Metropolis–Hastings Markov chain is equal to the target distribution (under general conditions) is a consequence of the following result.

Theorem 3.1: Local Balance for the Metropolis–Hastings Sampler

The transition density of the Metropolis–Hastings Markov chain satisfies the detailed balance equations.

☞ 455

Proof: We prove the theorem for the discrete case only. Because a transition of the Metropolis–Hastings Markov chain consists of two steps, the one-step transition probability to go from $\boldsymbol{x}$ to $\boldsymbol{y}$ is not $q(\boldsymbol{y} \,|\, \boldsymbol{x})$ but

$$\widetilde{q}(\boldsymbol{y} \,|\, \boldsymbol{x}) = \begin{cases} q(\boldsymbol{y} \,|\, \boldsymbol{x})\, \alpha(\boldsymbol{x}, \boldsymbol{y}), & \text{if } \boldsymbol{y} \neq \boldsymbol{x}, \\ 1 - \sum_{z \neq \boldsymbol{x}} q(z \,|\, \boldsymbol{x})\, \alpha(\boldsymbol{x}, z), & \text{if } \boldsymbol{y} = \boldsymbol{x}. \end{cases} \tag{3.5}$$

We thus need to show that

$$f(\boldsymbol{x})\, \widetilde{q}(\boldsymbol{y} \,|\, \boldsymbol{x}) = f(\boldsymbol{y})\, \widetilde{q}(\boldsymbol{x} \,|\, \boldsymbol{y}) \quad \text{for all } \boldsymbol{x}, \boldsymbol{y}. \tag{3.6}$$

With the acceptance probability as in (3.4), we need to check (3.6) for three cases:

(a) $\boldsymbol{x} = \boldsymbol{y}$,

(b) $\boldsymbol{x} \neq \boldsymbol{y}$ and $f(\boldsymbol{y}) q(\boldsymbol{x} \,|\, \boldsymbol{y}) \leqslant f(\boldsymbol{x}) q(\boldsymbol{y} \,|\, \boldsymbol{x})$, and

(c) $\boldsymbol{x} \neq \boldsymbol{y}$ and $f(\boldsymbol{y}) q(\boldsymbol{x} \,|\, \boldsymbol{y}) > f(\boldsymbol{x}) q(\boldsymbol{y} \,|\, \boldsymbol{x})$.

Case (a) holds trivially. For case (b), $\alpha(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{y}) q(\boldsymbol{x} \,|\, \boldsymbol{y}) / (f(\boldsymbol{x}) q(\boldsymbol{y} \,|\, \boldsymbol{x}))$ and $\alpha(\boldsymbol{y}, \boldsymbol{x}) = 1$. Consequently,

$$\widetilde{q}(\boldsymbol{y} \,|\, \boldsymbol{x}) = f(\boldsymbol{y}) q(\boldsymbol{x} \,|\, \boldsymbol{y}) / f(\boldsymbol{x}) \quad \text{and} \quad \widetilde{q}(\boldsymbol{x} \,|\, \boldsymbol{y}) = q(\boldsymbol{x} \,|\, \boldsymbol{y}),$$

so that (3.6) holds. Similarly, for case (c) we have $\alpha(\boldsymbol{x}, \boldsymbol{y}) = 1$ and $\alpha(\boldsymbol{y}, \boldsymbol{x}) = f(\boldsymbol{x}) q(\boldsymbol{y} \,|\, \boldsymbol{x}) / (f(\boldsymbol{y}) q(\boldsymbol{x} \,|\, \boldsymbol{y}))$. It follows that,

$$\widetilde{q}(\boldsymbol{y} \,|\, \boldsymbol{x}) = q(\boldsymbol{y} \,|\, \boldsymbol{x}) \quad \text{and} \quad \widetilde{q}(\boldsymbol{x} \,|\, \boldsymbol{y}) = f(\boldsymbol{x}) q(\boldsymbol{y} \,|\, \boldsymbol{x}) / f(\boldsymbol{y}),$$

so that (3.6) holds again. □

Thus if the Metropolis–Hastings Markov chain is ergodic, then its limiting pdf is $f(\boldsymbol{x})$. ☞ 454
A fortunate property of the algorithm, which is important in many applications, is that in order to evaluate the acceptance probability $\alpha(\boldsymbol{x}, \boldsymbol{y})$ in (3.4), one only needs to know the target pdf $f(\boldsymbol{x})$ *up to a constant*; that is $f(\boldsymbol{x}) = c\, \overline{f}(\boldsymbol{x})$ for some known function $\overline{f}(\boldsymbol{x})$ but unknown constant c.

The efficiency of the algorithm depends of course on the choice of the proposal transition density $q(\boldsymbol{y} \,|\, \boldsymbol{x})$. Ideally, we would like $q(\boldsymbol{y} \,|\, \boldsymbol{x})$ to be "close" to the target $f(\boldsymbol{y})$, irrespective of $\boldsymbol{x}$. We discuss two common approaches.

1. Choose the proposal transition density $q(\boldsymbol{y} \,|\, \boldsymbol{x})$ independent of $\boldsymbol{x}$; that is, $q(\boldsymbol{y} \,|\, \boldsymbol{x}) = g(\boldsymbol{y})$ for some pdf $g(\boldsymbol{y})$. An MCMC sampler of this type is called an *independence sampler*. The acceptance probability is thus

INDEPENDENCE SAMPLER

$$\alpha(\boldsymbol{x}, \boldsymbol{y}) = \min \left\{ \frac{f(\boldsymbol{y})\, g(\boldsymbol{x})}{f(\boldsymbol{x})\, g(\boldsymbol{y})},\ 1 \right\}.$$

2. If the proposal transition density is symmetric (that is, $q(\boldsymbol{y} \,|\, \boldsymbol{x}) = q(\boldsymbol{x} \,|\, \boldsymbol{y})$), then the acceptance probability has the simple form

$$\alpha(\boldsymbol{x}, \boldsymbol{y}) = \min\left\{\frac{f(\boldsymbol{y})}{f(\boldsymbol{x})},\ 1\right\}, \tag{3.7}$$

RANDOM WALK SAMPLER

and the MCMC algorithm is called a *random walk sampler*. A typical example is when, for a given current state $\boldsymbol{x}$, the proposal state $\boldsymbol{Y}$ is of the form $\boldsymbol{Y} = \boldsymbol{x} + \boldsymbol{Z}$, where $\boldsymbol{Z}$ is generated from some spherically symmetric distribution, such as $\mathcal{N}(\mathbf{0}, \mathbf{I})$.

We now give an example illustrating the second approach.

■ **Example 3.8 (Random Walk Sampler)** Consider the two-dimensional pdf

$$f(x_1, x_2) = c\, \mathrm{e}^{-\frac{1}{4}\sqrt{x_1^2+x_2^2}} \left(\sin\left(2\sqrt{x_1^2 + x_2^2}\right) + 1\right), \quad -2\pi < x_1 < 2\pi,\ -2\pi < x_2 < 2\pi, \tag{3.8}$$

where c is an unknown normalization constant. The graph of this pdf (unnormalized) is depicted in the left panel of Figure 3.5.

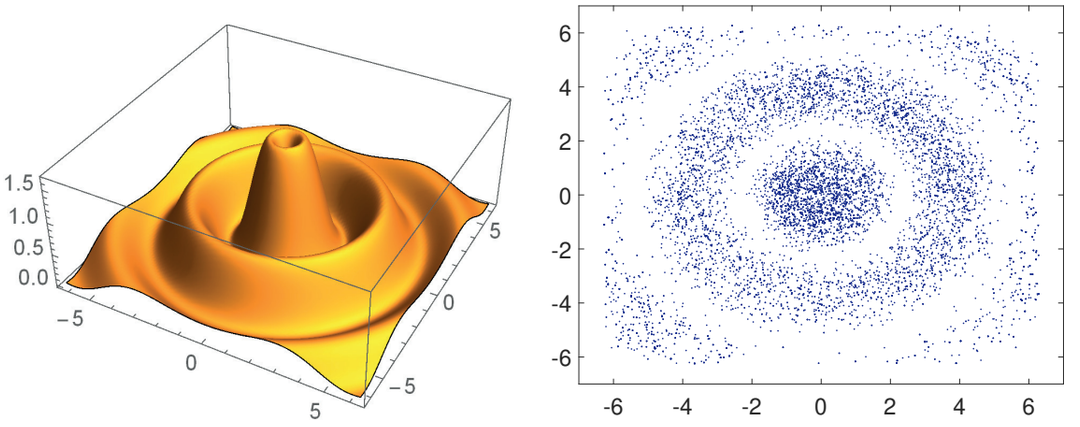


Figure 3.5: Left panel: the two-dimensional target pdf. Right panel: points from the random walk sampler are approximately distributed according to the target pdf.

The following Python program implements a random walk sampler to (approximately) draw $N = 10^4$ dependent samples from the pdf f. At each step, given a current state $\boldsymbol{x}$, a proposal $\boldsymbol{Y}$ is drawn from the $\mathcal{N}(\boldsymbol{x}, \mathbf{I})$ distribution. That is, $\boldsymbol{Y} = \boldsymbol{x} + \boldsymbol{Z}$, with $\boldsymbol{Z}$ bivariate standard normal. We see in the right panel of Figure 3.5 that the sampler works correctly. The starting point for the Markov chain is chosen as $(0, 0)$. Note that the normalization constant c is never required to be specified in the program.

rwsamp.py

```
import numpy as np
import matplotlib.pyplot as plt
from numpy import pi, exp, sqrt, sin
from numpy.random import rand, randn
```

```
N = 10000
a = lambda x: -2*pi < x
b = lambda x: x < 2*pi
f = lambda x1, x2: exp(-sqrt(x1**2+x2**2)/4)*(
        sin(2*sqrt(x1**2+x2**2))+1)*a(x1)*b(x1)*a(x2)*b(x2)

xx = np.zeros((N,2))
x = np.zeros((1,2))
for i in range(1,N):
    y = x + randn(1,2)
    alpha = np.amin((f(y[0][0],y[0][1])/f(x[0][0],x[0][1]),1))
    r = rand() < alpha
    x = r*y + (1-r)*x
    xx[i,:] = x

plt.scatter(xx[:,0], xx[:,1], alpha =0.4,s =2)
plt.axis('equal')
plt.show()
```

3.2.5.2 Gibbs Sampler

GIBBS SAMPLER

The *Gibbs sampler* [48] uses a somewhat different methodology from the Metropolis–Hastings algorithm and is particularly useful for generating n-dimensional random vectors. The key idea of the Gibbs sampler is to update the components of the random vector one at a time, by sampling them from *conditional* pdfs. Thus, Gibbs sampling can be advantageous if it is easier to sample from the conditional distributions than from the joint distribution.

Specifically, suppose that we wish to sample a random vector $\boldsymbol{X} = [X_1, \ldots, X_n]^\top$ according to a target pdf $f(\boldsymbol{x})$. Let $f(x_i \,|\, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ represent the conditional pdf[2] of the i-th component, X_i, given the other components $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$. The Gibbs sampling algorithm is as follows.

Algorithm 3.2.8: Gibbs Sampler

input: Initial point $\boldsymbol{X}_0$, sample size N, and target pdf f.
output: $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$ approximately distributed according to f.

for $t = 0$ **to** $N - 1$ **do**
  Draw Y_1 from the conditional pdf $f(y_1 \,|\, X_{t,2}, \ldots, X_{t,n})$.
  for $i = 2$ **to** n **do**
    Draw Y_i from the conditional pdf $f(y_i \,|\, Y_1, \ldots, Y_{i-1}, X_{t,i+1}, \ldots, X_{t,n})$.
  $\boldsymbol{X}_{t+1} \leftarrow \boldsymbol{Y}$
return $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$

There exist many variants of the Gibbs sampler, depending on the steps required to update $\boldsymbol{X}_t$ to $\boldsymbol{X}_{t+1}$ — called the *cycle* of the Gibbs algorithm. In the algorithm above, the

CYCLE

[2] In this section we employ a Bayesian notation style, using the same letter f for different (conditional) densities.

cycle consists of Steps 2–5, in which the components are updated in a fixed order $1 \to 2 \to \cdots \to n$. For this reason Algorithm 3.2.8 is also called the *systematic Gibbs sampler*.

SYSTEMATIC GIBBS SAMPLER

In the *random-order Gibbs sampler*, the order in which the components are updated in each cycle is a random permutation of $\{1, \ldots, n\}$ (see Exercise 9). Other modifications are to update the components in blocks (i.e., several at the same time), or to update only a random selection of components. The variant where in each cycle only a single random component is updated is called the *random Gibbs sampler*. In the *reversible Gibbs sampler* a cycle consists of the coordinate-wise updating $1 \to 2 \to \cdots \to n-1 \to n \to n-1 \to \cdots \to 2 \to 1$. In all cases, except for the systematic Gibbs sampler, the resulting Markov chain $\{\boldsymbol{X}_t, t = 1, 2, \ldots\}$ is *reversible* and hence its limiting distribution is precisely $f(\boldsymbol{x})$.

RANDOM-ORDER GIBBS SAMPLER

☞ 115

RANDOM GIBBS SAMPLER

REVERSIBLE GIBBS SAMPLER

☞ 454

Unfortunately, the systematic Gibbs Markov chain is not reversible and so the detailed balance equations are not satisfied. However, a similar result holds, due to Hammersley and Clifford, under the so-called *positivity condition*: if at a point $\boldsymbol{x} = (x_1, \ldots, x_n)$ all marginal densities $f(x_i) > 0, i = 1, \ldots, n$, then the joint density $f(\boldsymbol{x}) > 0$.

Theorem 3.2: Hammersley–Clifford Balance for the Gibbs Sampler

Let $q_{1\to n}(\boldsymbol{y} \,|\, \boldsymbol{x})$ denote the transition density of the systematic Gibbs sampler, and let $q_{n\to 1}(\boldsymbol{x} \,|\, \boldsymbol{y})$ be the transition density of the reverse move, in the order $n \to n-1 \to \cdots \to 1$. Then, if the positivity condition holds,

$$f(\boldsymbol{x})\, q_{1\to n}(\boldsymbol{y} \,|\, \boldsymbol{x}) = f(\boldsymbol{y})\, q_{n\to 1}(\boldsymbol{x} \,|\, \boldsymbol{y}). \tag{3.9}$$

Proof: For the forward move we have:

$$q_{1\to n}(\boldsymbol{y} \,|\, \boldsymbol{x}) = f(y_1 \,|\, x_2, \ldots, x_n) f(y_2 \,|\, y_1, x_3, \ldots, x_n) \cdots f(y_n \,|\, y_1, \ldots, y_{n-1}),$$

and for the reverse move:

$$q_{n\to 1}(\boldsymbol{x} \,|\, \boldsymbol{y}) = f(x_n \,|\, y_1, \ldots, y_{n-1}) f(x_{n-1} \,|\, y_1, \ldots, y_{n-2}, x_n) \cdots f(x_1 \,|\, x_2, \ldots, x_n).$$

Consequently,

$$\begin{aligned}
\frac{q_{1\to n}(\boldsymbol{y} \,|\, \boldsymbol{x})}{q_{n\to 1}(\boldsymbol{x} \,|\, \boldsymbol{y})} &= \prod_{i=1}^{n} \frac{f(y_i \,|\, y_1, \ldots, y_{i-1}, x_{i+1}, \ldots, x_n)}{f(x_i \,|\, y_1, \ldots, y_{i-1}, x_{i+1}, \ldots, x_n)} \\
&= \prod_{i=1}^{n} \frac{f(y_1, \ldots, y_i, x_{i+1}, \ldots, x_n)}{f(y_1, \ldots, y_{i-1}, x_i, \ldots, x_n)} \\
&= \frac{f(\boldsymbol{y}) \prod_{i=1}^{n-1} f(y_1, \ldots, y_i, x_{i+1}, \ldots, x_n)}{f(\boldsymbol{x}) \prod_{j=2}^{n} f(y_1, \ldots, y_{j-1}, x_j, \ldots, x_n)} \\
&= \frac{f(\boldsymbol{y}) \prod_{i=1}^{n-1} f(y_1, \ldots, y_i, x_{i+1}, \ldots, x_n)}{f(\boldsymbol{x}) \prod_{j=1}^{n-1} f(y_1, \ldots, y_j, x_{j+1}, \ldots, x_n)} = \frac{f(\boldsymbol{y})}{f(\boldsymbol{x})}.
\end{aligned}$$

The result follows by rearranging the last identity. The positivity condition ensures that we do not divide by 0 along the line. □

Intuitively, the long-run proportion of transitions $\boldsymbol{x} \to \boldsymbol{y}$ for the "forward move" chain is equal to the long-run proportion of transitions $\boldsymbol{y} \to \boldsymbol{x}$ for the "reverse move" chain.

To verify that the Markov chain $\boldsymbol{X}_0, \boldsymbol{X}_1, \ldots$ for the systematic Gibbs sampler indeed has limiting pdf $f(\boldsymbol{x})$, we need to check that the global balance equations (C.42) hold. By integrating (in the continuous case) both sides in (3.9) with respect to $\boldsymbol{x}$, we see that indeed ☞ 454

$$\int f(\boldsymbol{x})\, q_{1\to n}(\boldsymbol{y} \,|\, \boldsymbol{x})\, \mathrm{d}\boldsymbol{x} = f(\boldsymbol{y}).$$

■ **Example 3.9 (Gibbs Sampler for the Bayesian Normal Model)** Gibbs samplers are often applied in Bayesian statistics, to sample from the posterior pdf. Consider for instance the Bayesian normal model ☞ 50

$$\begin{aligned} f(\mu, \sigma^2) &= 1/\sigma^2 \\ (\boldsymbol{x} \,|\, \mu, \sigma^2) &\sim \mathcal{N}(\mu \mathbf{1}, \sigma^2 \mathbf{I}). \end{aligned}$$

Here the prior for (μ, σ^2) is *improper*. That is, it is not a pdf in itself, but by obstinately applying Bayes' formula it does yield a proper posterior pdf. In some sense this prior conveys the least amount of information about μ and σ^2. Following the same procedure as in Example 2.8, we find the posterior pdf: IMPROPER PRIOR

$$f(\mu, \sigma^2 \,|\, \boldsymbol{x}) \propto \left(\sigma^2\right)^{-n/2-1} \exp\left\{-\frac{1}{2}\frac{\sum_i (x_i - \mu)^2}{\sigma^2}\right\}. \tag{3.10}$$

Note that μ and σ^2 here are the "variables" and $\boldsymbol{x}$ is a fixed data vector. To simulate samples μ and σ^2 from (3.10) using the Gibbs sampler, we need the distributions of both $(\mu \,|\, \sigma^2, \boldsymbol{x})$ and $(\sigma^2 \,|\, \mu, \boldsymbol{x})$. To find $f(\mu \,|\, \sigma^2, \boldsymbol{x})$, view the right-hand side of (3.10) as a function of μ only, regarding σ^2 as a constant. This gives

$$\begin{aligned} f(\mu \,|\, \sigma^2, \boldsymbol{x}) &\propto \exp\left\{-\frac{n\mu^2 - 2\mu \sum_i x_i}{2\sigma^2}\right\} = \exp\left\{-\frac{\mu^2 - 2\mu\bar{x}}{2(\sigma^2/n)}\right\} \\ &\propto \exp\left\{-\frac{1}{2}\frac{(\mu - \bar{x})^2}{\sigma^2/n}\right\}. \end{aligned} \tag{3.11}$$

This shows that $(\mu \,|\, \sigma^2, \boldsymbol{x})$ has a normal distribution with mean $\bar{x}$ and variance σ^2/n.

Similarly, to find $f(\sigma^2 \,|\, \mu, \boldsymbol{x})$, view the right-hand side of (3.10) as a function of σ^2, regarding μ as a constant. This gives

$$f(\sigma^2 \,|\, \mu, \boldsymbol{x}) \propto (\sigma^2)^{-n/2-1} \exp\left\{-\frac{1}{2}\sum_{i=1}^{n}(x_i - \mu)^2/\sigma^2\right\}, \tag{3.12}$$

showing that $(\sigma^2 \,|\, \mu, \boldsymbol{x})$ has an inverse-gamma distribution with parameters $n/2$ and $\sum_{i=1}^n (x_i - \mu)^2/2$. The Gibbs sampler thus involves the repeated simulation of ☞ 427

$$(\mu \,|\, \sigma^2, \boldsymbol{x}) \sim \mathcal{N}\left(\bar{x},\ \sigma^2/n\right) \quad \text{and} \quad (\sigma^2 \,|\, \mu, \boldsymbol{x}) \sim \mathsf{InvGamma}\left(n/2,\ \sum_{i=1}^{n}(x_i - \mu)^2/2\right).$$

Simulating $X \sim \mathsf{InvGamma}(\alpha, \lambda)$ is achieved by first generating $Z \sim \mathsf{Gamma}(\alpha, \lambda)$ and then returning $X = 1/Z$.

In our parameterization of the Gamma(α, λ) distribution, λ is the *rate* parameter. Many software packages instead use the *scale* parameter $c = 1/\lambda$. Be aware of this when simulating Gamma random variables.

The Python script below defines a small data set of size $n = 10$ (which was randomly simulated from a standard normal distribution), and implements the systematic Gibbs sampler to simulate from the posterior distribution, using $N = 10^5$ samples.

gibbsamp.py

```
import numpy as np
import matplotlib.pyplot as plt

x = np.array([[-0.9472, 0.5401, -0.2166, 1.1890, 1.3170,
               -0.4056, -0.4449, 1.3284, 0.8338, 0.6044]])
n=x.size
sample_mean = np.mean(x)
sample_var = np.var(x)
sig2 = np.var(x)
mu=sample_mean

N=10**5
gibbs_sample = np.array(np.zeros((N, 2)))
for k in range(N):
    mu=sample_mean + np.sqrt(sig2/n)*np.random.randn()
    V=np.sum((x-mu)**2)/2
    sig2 = 1/np.random.gamma(n/2, 1/V)
    gibbs_sample[k,:]= np.array([mu, sig2])
plt.scatter(gibbs_sample[:,0], gibbs_sample[:,1],alpha =0.1,s =1)
plt.plot(np.mean(x), np.var(x),'wo')
plt.show()
```

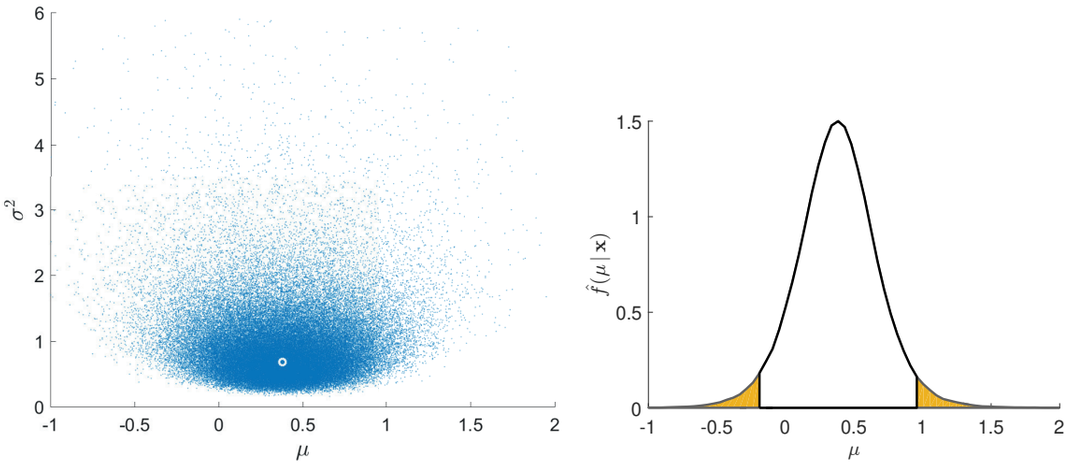


Figure 3.6: Left: approximate draws from the posterior pdf $f(\mu, \sigma^2 \,|\, \boldsymbol{x})$ obtained via the Gibbs sampler. Right: estimate of the posterior pdf $f(\mu \,|\, \boldsymbol{x})$.

The left panel of Figure 3.6 shows the (μ, σ^2) points generated by the Gibbs sampler. Also shown, via the white circle, is the point $(\overline{x}, s^2)$, where $\overline{x} = 0.3798$ is the sample mean and $s^2 = 0.6810$ the sample variance. This posterior point cloud visualizes the considerable uncertainty in the estimates. By projecting the (μ, σ^2) points onto the μ-axis — that is, by ignoring the σ^2 values — one obtains (approximate) samples from the posterior pdf of μ; that is, $f(\mu \,|\, \boldsymbol{x})$. The right panel of Figure 3.6 shows a kernel density estimate (see Section 4.4) of this pdf. The corresponding 0.025 and 0.975 sample quantiles were found to be -0.2054 and 0.9662, respectively, giving the 95% credible interval $(-0.2054, 0.9662)$ for μ, which contains the true expectation 0. Similarly, an estimated 95% credible interval for σ^2 is $(0.3218, 2.2485)$, which contains the true variance 1.

☞ 134

3.3 Monte Carlo Estimation

In this section we describe how Monte Carlo simulation can be used to estimate complicated integrals, probabilities, and expectations. A number of variance reduction techniques are introduced as well, including the recent cross-entropy method.

3.3.1 Crude Monte Carlo

The most common setting for Monte Carlo estimation is the following: Suppose we wish to compute the expectation $\mu = \mathbb{E}Y$ of some (say continuous) random variable Y with pdf f, but the integral $\mathbb{E}Y = \int y f(y)\, \mathrm{d}y$ is difficult to evaluate. For example, if Y is a complicated function of other random variables, it would be difficult to obtain an exact expression for $f(y)$. The idea of *crude Monte Carlo* — sometimes abbreviated as CMC — is to approximate μ by simulating many independent copies $Y_1, \ldots, Y_N$ of Y and then take their *sample mean* $\overline{Y}$ as an estimator of μ. All that is needed is an algorithm to simulate such copies.

CRUDE MONTE CARLO

By the Law of Large Numbers, $\overline{Y}$ converges to μ as $N \to \infty$, provided the expectation of Y exists. Moreover, by the Central Limit Theorem, $\overline{Y}$ approximately has a $\mathcal{N}(\mu, \sigma^2/N)$ distribution for large N, provided that the variance $\sigma^2 = \mathbb{V}\mathrm{ar}Y < \infty$. This enables the construction of an approximate $(1 - \alpha)$ *confidence interval* for μ:

☞ 448
☞ 449

CONFIDENCE INTERVAL

$$\left(\overline{Y} - z_{1-\alpha/2} \frac{S}{\sqrt{N}}, \quad \overline{Y} + z_{1-\alpha/2} \frac{S}{\sqrt{N}} \right), \tag{3.13}$$

where S is the sample standard deviation of the $\{Y_i\}$ and z_γ denotes the γ-quantile of the $\mathcal{N}(0, 1)$ distribution; see also Section C.13. Instead of specifying the confidence interval, one often reports only the sample mean and the *estimated standard error*: $S/\sqrt{N}$, or the *estimated relative error*: $S/(\overline{Y}\sqrt{N})$. The basic estimation procedure for independent data is summarized in Algorithm 3.3.1 below.

☞ 459

ESTIMATED STANDARD ERROR

ESTIMATED RELATIVE ERROR

It is often the case that the output Y is a function of some underlying random vector or stochastic process; that is, $Y = H(\boldsymbol{X})$, where H is a real-valued function and $\boldsymbol{X}$ is a random vector or process. The beauty of Monte Carlo for estimation is that (3.13) holds regardless of the dimension of $\boldsymbol{X}$.

Algorithm 3.3.1: Crude Monte Carlo for Independent Data

input: Simulation algorithm for $Y \sim f$, sample size N, confidence level $1-\alpha$.
output: Point estimate and approximate $(1-\alpha)$ confidence interval for $\mu = \mathbb{E}Y$.

1 Simulate $Y_1, \ldots, Y_N \overset{\text{iid}}{\sim} f$.
2 $\overline{Y} \leftarrow \frac{1}{N}\sum_{i=1}^{N} Y_i$
3 $S^2 \leftarrow \frac{1}{N-1}\sum_{i=1}^{N}(Y_i - \overline{Y})^2$
4 **return** $\overline{Y}$ and the interval (3.13).

MONTE CARLO INTEGRATION

■ **Example 3.10 (Monte Carlo Integration)** In *Monte Carlo integration*, simulation is used to evaluate complicated integrals. Consider, for example, the integral

$$\mu = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \sqrt{|x_1 + x_2 + x_3|}\, \mathrm{e}^{-(x_1^2+x_2^2+x_3^2)/2}\, \mathrm{d}x_1\, \mathrm{d}x_2\, \mathrm{d}x_3.$$

Defining $Y = |X_1 + X_2 + X_3|^{1/2}(2\pi)^{3/2}$, with $X_1, X_2, X_3 \overset{\text{iid}}{\sim} \mathcal{N}(0,1)$, we can write $\mu = \mathbb{E}Y$. Using the following Python program, with a sample size of $N = 10^6$, we obtained an estimate $\overline{Y} = 17.031$ with an approximate 95% confidence interval $(17.017, 17.046)$.

mcint.py

```
import numpy as np
from numpy import pi

c = (2*pi)**(3/2)
H = lambda x: c*np.sqrt(np.abs(np.sum(x,axis=1)))
N = 10**6
z = 1.96
x = np.random.randn(N,3)
y = H(x)
mY = np.mean(y)
sY = np.std(y)
RE = sY/mY/np.sqrt(N)
print('Estimate = {:3.3f}, CI = ({:3.3f},{:3.3f})'.format(
        mY, mY*(1-z*RE), mY*(1+z*RE)))
```

```
Estimate = 17.031, CI = (17.017,17.046)
```

■

■ **Example 3.11 (Example 2.1 (cont.))** We return to the bias–variance tradeoff in Example 2.1. Figure 2.7 gives estimates of the (squared-error) generalization risk (2.5) as a function of the number of parameters in the model. But how accurate are these estimates? Because we know in this case the exact model for the data, we can use Monte Carlo simulation to estimate the generalization risk (for a fixed training set) and the expected generalization risk (averaged over all training sets) precisely. All we need to do is repeat the data generation, fitting, and validation steps many times and then take averages of the results. The following Python code repeats 100 times:

☞ 26
☞ 29
☞ 23

1. Simulate the training set of size $n = 100$.
2. Fit models up to size $k = 8$.

3. Estimate the test loss using a test set with the same sample size $n = 100$.

Figure 3.7 shows that there is some variation in the test losses, due to the randomness in both the training and test sets. To obtain an accurate estimate of the expected generalization risk (2.6), take the average of the test losses. We see that for $k \leqslant 8$ the estimate in Figure 2.7 is close to the true expected generalization risk.

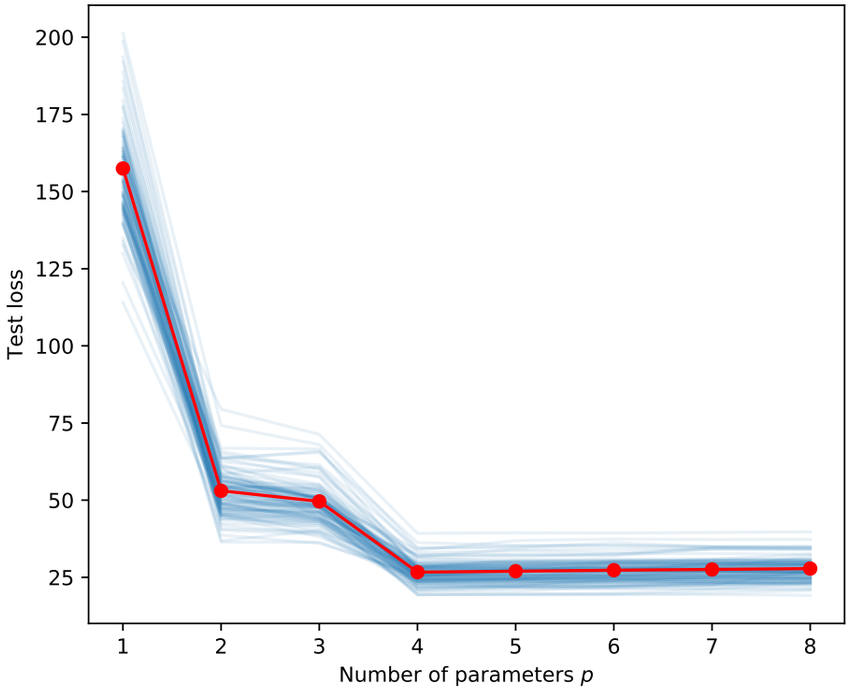


Figure 3.7: Independent estimates of the test loss show some variability.

CMCtestloss.py

```
import numpy as np, matplotlib.pyplot as plt
from numpy.random import rand, randn
from numpy.linalg import solve

def generate_data(beta, sig, n):
    u = rand(n, 1)
    y = (u ** np.arange(0, 4)) @ beta + sig * randn(n, 1)
    return u, y

beta = np.array([[10, -140, 400, -250]]).T
n = 100
sig = 5
betahat = {}
plt.figure(figsize=[6,5])
totMSE = np.zeros(8)
max_p = 8
p_range = np.arange(1, max_p + 1, 1)

for N in range(0,100):
```

```
    u, y = generate_data(beta, sig, n)  #training data
    X = np.ones((n, 1))
    for p in p_range:
       if p > 1:
         X = np.hstack((X, u**(p-1)))
       betahat[p] = solve(X.T @ X, X.T @ y)

    u_test, y_test = generate_data(beta, sig, n)  #test data
    MSE = []
    X_test = np.ones((n, 1))
    for p in p_range:
       if p > 1:
           X_test = np.hstack((X_test, u_test**(p-1)))
       y_hat = X_test @ betahat[p] # predictions
       MSE.append(np.sum((y_test - y_hat)**2/n))

    totMSE = totMSE + np.array(MSE)
    plt.plot(p_range, MSE,'C0',alpha=0.1)

plt.plot(p_range,totMSE/N,'r-o')
plt.xticks(ticks=p_range)
plt.xlabel('Number of parameters $p$')
plt.ylabel('Test loss')
plt.tight_layout()
plt.savefig('MSErepeatpy.pdf',format='pdf')
plt.show()
```

■

3.3.2 Bootstrap Method

The bootstrap method [37] combines CMC estimation with the resampling procedure of
☞ 76
Section 3.2.4. The idea is as follows: Suppose we wish to estimate a number μ via some estimator $Y = H(\mathcal{T})$, where $\mathcal{T} := \{X_1, \ldots, X_n\}$ is an iid sample from some unknown cdf F. It is assumed that Y does not depend on the order of the $\{X_i\}$. To assess the quality (for example, accuracy) of the estimator Y, one could draw independent replications $\mathcal{T}_1, \ldots, \mathcal{T}_N$ of $\mathcal{T}$ and find sample estimates for quantities such as the variance $\mathbb{V}\mathrm{ar}Y$, the bias $\mathbb{E}Y - \mu$, and the mean squared error $\mathbb{E}(Y - \mu)^2$. However, it may be too time-consuming or simply not feasible to obtain such replications. An alternative is to *resample* the original data. To reiterate, given an outcome $\tau = \{x_1, \ldots, x_n\}$ of $\mathcal{T}$, we simulate an iid sample $\mathcal{T}^* := \{X_1^*, \ldots, X_n^*\}$ from the empirical cdf F_n, via Algorithm 3.2.6 (hence the resampling size is $N = n$ here).
☞ 76

The rationale is that the empirical cdf F_n is close to the actual cdf F and gets closer as n gets larger. Hence, any quantities depending on F, such as $\mathbb{E}_F g(Y)$, where g is a function, can be approximated by $\mathbb{E}_{F_n} g(Y)$. The latter is usually still difficult to evaluate, but it can be simply estimated via CMC as

$$\frac{1}{K} \sum_{i=1}^{K} g(Y_i^*),$$

where $Y_1^*, \ldots, Y_K^*$ are independent random variables, each distributed as $Y^* = H(\mathcal{T}^*)$. This seemingly self-referent procedure is called *bootstrapping* — alluding to Baron von Mün-

BOOTSTRAPPING

chausen, who pulled himself out of a swamp by his own bootstraps. As an example, the bootstrap estimate of the expectation of Y is

$$\widehat{\mathbb{E}Y} = \overline{Y}^* = \frac{1}{K}\sum_{i=1}^{K} Y_i^*,$$

which is simply the sample mean of $\{Y_i^*\}$. Similarly, the bootstrap estimate for $\mathbb{V}\mathrm{ar}Y$ is the sample variance

$$\widehat{\mathbb{V}\mathrm{ar}Y} = \frac{1}{K-1}\sum_{i=1}^{K}(Y_i^* - \overline{Y}^*)^2. \tag{3.14}$$

Bootstrap estimators for the bias and MSE are $\overline{Y}^* - Y$ and $\frac{1}{K}\sum_{i=1}^{K}(Y_i^* - Y)^2$, respectively. Note that for these estimators the unknown quantity μ is replaced with its original estimator Y. Confidence intervals can be constructed in the same fashion. We mention two variants: the *normal method* and the *percentile method*. In the normal method, a $1-\alpha$ confidence interval for μ is given by

NORMAL METHOD
PERCENTILE METHOD

$$(Y \pm z_{1-\alpha/2} S^*),$$

where S^* is the bootstrap estimate of the standard deviation of Y; that is, the square root of (3.14). In the percentile method, the upper and lower bounds of the $1-\alpha$ confidence interval for μ are given by the $1-\alpha/2$ and $\alpha/2$ quantiles of Y, which in turn are estimated via the corresponding sample quantiles of the bootstrap sample $\{Y_i^*\}$.

The following example illustrates the usefulness of the bootstrap method for *ratio estimation* and also introduces the *renewal reward process* model for data.

■ **Example 3.12 (Bootstrapping the Ratio Estimator)** A common scenario in stochastic simulation is that the output of the simulation consists of independent pairs of data $(C_1, R_1), (C_2, R_2), \ldots$, where each C is interpreted as the length of a period of time — a so-called *cycle* — and R is the *reward* obtained during that cycle. Such a collection of random variables $\{(C_i, R_i)\}$ is called a *renewal reward process*. Typically, the reward R_i depends on the cycle length C_i. Let A_t be the *average reward* earned by time t; that is, $A_t = \sum_{i=1}^{N_t} R_i/t$, where $N_t = \max\{n : C_1 + \cdots + C_n \leqslant t\}$ counts the number of complete cycles at time t. It can be shown, see Exercise 20, that if the expectations of the cycle length and reward are finite, then A_t converges to the constant $\mathbb{E}R/\mathbb{E}C$. This ratio can thus be interpreted as the *long-run average reward*.

RENEWAL REWARD PROCESS

☞ 118

LONG-RUN AVERAGE REWARD

Estimation of the ratio $\mathbb{E}R/\mathbb{E}C$ from data $(C_1, R_1), \ldots, (C_n, R_n)$ is easy: take the *ratio estimator*

RATIO ESTIMATOR

$$A = \frac{\overline{R}}{\overline{C}}.$$

However, this estimator A is not unbiased and it is not obvious how to derive confidence intervals. Fortunately, the bootstrap method can come to the rescue: simply resample the pairs $\{(C_i, R_i)\}$, obtain ratio estimators $A_1^*, \ldots, A_K^*$, and from these compute quantities of interest such as confidence intervals.

As a concrete example, let us return to the Markov chain in Example 3.6. Recall that the chain starts at state 1 at time 0. After a certain amount of time T_1, the process returns to state 1. The time steps $0, \ldots, T_1 - 1$ form a natural "cycle" for this process, as from time T_1 onwards the process behaves probabilistically *exactly the same* as when it started,

☞ 75

independently of $X_0, \ldots, X_{T_1-1}$. Thus, if we define $T_0 = 0$, and let T_i be the i-th time that the chain returns to state 1, then we can break up the time interval into independent cycles of lengths $C_i = T_i - T_{i-1}$, $i = 1, 2, \ldots$. Now suppose that during the i-th cycle a reward

$$R_i = \sum_{t=T_{i-1}}^{T_i-1} \varrho^{t-T_{i-1}} \, r(X_t)$$

is received, where $r(i)$ is some fixed reward for visiting state $i \in \{1, 2, 3, 4\}$ and $\varrho \in (0, 1)$ is a discounting factor. Clearly, $\{(C_i, R_i)\}$ is a renewal reward process. Figure 3.8 shows the outcomes of 1000 pairs (C, R), using $r(1) = 4$, $r(2) = 3$, $r(3) = 10$, $r(4) = 1$, and $\varrho = 0.9$.

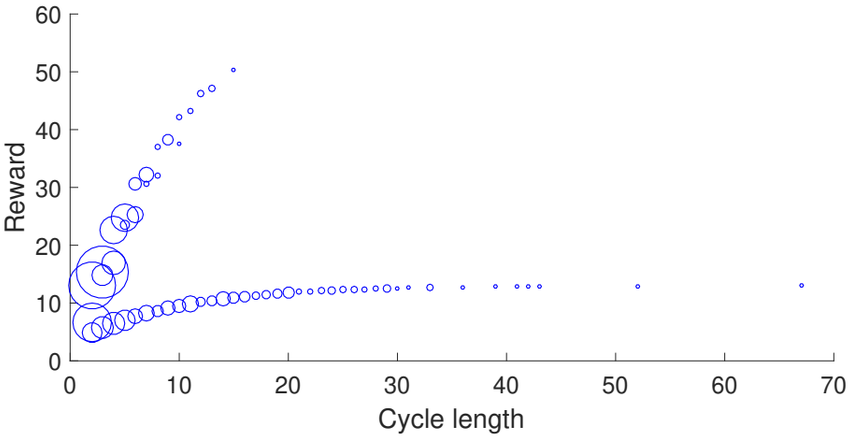


Figure 3.8: Each circle represents a (cycle length, reward) pair. The varying circle sizes indicate the number of occurrences for a given pair. For example, (2,15.43) is the most likely pair here, occurring 186 out of a 1000 times. It corresponds to the cycle path $1 \to 3 \to 2 \to 1$.

The long-run average reward is estimated as 2.50 for our data. But how accurate is this estimate? Figure 3.9 shows a density plot of the bootstrapped ratio estimates, where we independently resampled the data pairs 1000 times.

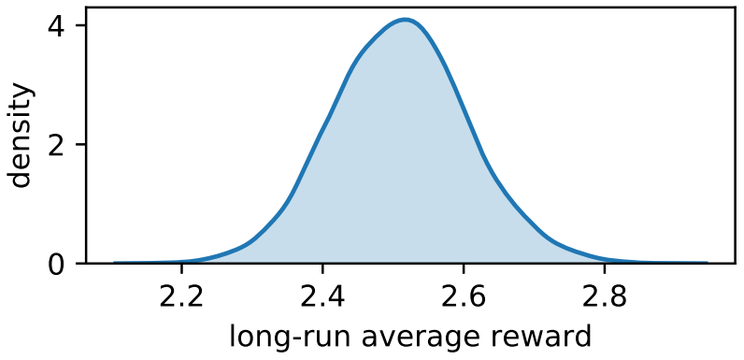


Figure 3.9: Density plot of the bootstrapped ratio estimates for the Markov chain renewal reward process.

Figure 3.9 indicates that the true long-run average reward lies between 2.2 and 2.8 with high confidence. More precisely, the 99% bootstrap confidence interval (percentile method) is here (2.27, 2.77). The following Python script spells out the procedure.

ratioest.py

```
import numpy as np, matplotlib.pyplot as plt, seaborn as sns
from numba import jit

np.random.seed(123)
n = 1000
P = np.array([[0, 0.2, 0.5, 0.3],
              [0.5 ,0, 0.5, 0],
              [0.3, 0.7, 0, 0],
              [0.1, 0, 0, 0.9]])
r = np.array([4,3,10,1])
Corg = np.array(np.zeros((n,1)))
Rorg = np.array(np.zeros((n,1)))
rho=0.9

@jit()   #for speed-up; see Appendix
def generate_cyclereward(n):
   for i in range(n):
       t=1
       xreg = 1   #regenerative state  (out of 1,2,3,4)
       reward = r[0]
       x= np.amin(np.argwhere(np.cumsum(P[xreg-1,:]) > np.random.
          rand())) + 1
       while x != xreg:
           t += 1
           reward += rho**(t-1)*r[x-1]
           x = np.amin(np.where(np.cumsum(P[x-1,:]) > np.random.rand
              ())) + 1
       Corg[i] = t
       Rorg[i] = reward
   return Corg, Rorg

Corg, Rorg = generate_cyclereward(n)

Aorg = np.mean(Rorg)/np.mean(Corg)
K = 5000
A = np.array(np.zeros((K,1)))
C = np.array(np.zeros((n,1)))
R = np.array(np.zeros((n,1)))
for i in range(K):
    ind = np.ceil(n*np.random.rand(1,n)).astype(int)[0]-1
    C = Corg[ind]
    R = Rorg[ind]
    A[i] = np.mean(R)/np.mean(C)

plt.xlabel('long-run average reward')
plt.ylabel('density')
sns.kdeplot(A.flatten(),shade=True)
plt.show()
```

3.3.3 Variance Reduction

The estimation of performance measures in Monte Carlo simulation can be made more efficient by utilizing known information about the simulation model. Variance reduction techniques include antithetic variables, control variables, importance sampling, conditional Monte Carlo, and stratified sampling; see, for example, [71, Chapter 9]. We shall only deal with control variables and importance sampling here.

CONTROL VARIABLE

Suppose Y is the output of a simulation experiment. A random variable $\widetilde{Y}$, obtained from the same simulation run, is called a *control variable* for Y if Y and $\widetilde{Y}$ are correlated (negatively or positively) and the expectation of $\widetilde{Y}$ is known. The use of control variables for variance reduction is based on the following theorem. We leave its proof to Exercise 21.

☞ 118

Theorem 3.3: Control Variable Estimation

Let $Y_1, \ldots, Y_N$ be the output of N independent simulation runs and let $\widetilde{Y}_1, \ldots, \widetilde{Y}_N$ be the corresponding control variables, with $\mathbb{E}\widetilde{Y}_k = \widetilde{\mu}$ known. Let $\varrho_{Y,\widetilde{Y}}$ be the correlation coefficient between each Y_k and $\widetilde{Y}_k$. For each $\alpha \in \mathbb{R}$ the estimator

$$\widehat{\mu}^{(c)} = \frac{1}{N} \sum_{k=1}^{N} \left[Y_k - \alpha \left(\widetilde{Y}_k - \widetilde{\mu} \right) \right] \tag{3.15}$$

is an unbiased estimator for $\mu = \mathbb{E}Y$. The minimal variance of $\widehat{\mu}^{(c)}$ is

$$\mathbb{V}\mathrm{ar}\, \widehat{\mu}^{(c)} = \frac{1}{N} (1 - \varrho^2_{Y,\widetilde{Y}}) \, \mathbb{V}\mathrm{ar}\, Y, \tag{3.16}$$

which is obtained for $\alpha = \varrho_{Y,\widetilde{Y}} \sqrt{\mathbb{V}\mathrm{ar} Y / \mathbb{V}\mathrm{ar} \widetilde{Y}}$.

From (3.16) we see that, by using the optimal α in (3.15), the variance of the control variate estimator is a factor $1 - \varrho^2_{Y,\widetilde{Y}}$ smaller than the variance of the crude Monte Carlo estimator. Thus, if $\widetilde{Y}$ is highly correlated with Y, a significant variance reduction can be achieved. The optimal α is usually unknown, but it can be easily estimated from the sample covariance matrix of $\{(Y_k, \widetilde{Y}_k)\}$.

☞ 458

In the next example, we estimate the multiple integral in Example 3.10 using control variables.

☞ 86

■ **Example 3.13 (Monte Carlo Integration (cont.))** The random variable $Y = |X_1 + X_2 + X_3|^{1/2} (2\pi)^{3/2}$ is positively correlated with the random variable $\widetilde{Y} = X_1^2 + X_2^2 + X_3^2$, for the same choice of $X_1, X_2, X_3 \overset{\text{iid}}{\sim} \mathcal{N}(0, 1)$. As $\mathbb{E}\widetilde{Y} = \mathbb{V}\mathrm{ar}(X_1 + X_2 + X_3) = 3$, we can use it as a control variable to estimate the expectation of Y. The following Python program is based on Theorem 3.3. It imports the crude Monte Carlo sampling code from Example 3.10.

mcintCV.py

```
from mcint import *

Yc = np.sum(x**2, axis=1) # control variable data
yc = 3  # true expectation of control variable
C = np.cov(y,Yc) # sample covariance matrix
cor = C[0][1]/np.sqrt(C[0][0]*C[1][1])
alpha = C[0][1]/C[1][1]

est = np.mean(y-alpha*(Yc-yc))
RECV = np.sqrt((1-cor**2)*C[0][0]/N)/est  #relative error

print('Estimate = {:3.3f}, CI = ({:3.3f},{:3.3f}), Corr = {:3.3f}'.
      format(est, est*(1-z*RECV), est*(1+z*RECV),cor))
```

```
Estimate = 17.045, CI = (17.032,17.057), Corr = 0.480
```

A typical estimate of the correlation coefficient $\varrho_{Y,\widetilde{Y}}$ is 0.48, which gives a reduction of the variance with a factor $1-0.48^2 \approx 0.77$ — a simulation speed-up of 23% compared with crude Monte Carlo. Although the gain is small in this case, due to the modest correlation between Y and $\widetilde{Y}$, little extra work was required to achieve this variance reduction. ■

IMPORTANCE SAMPLING

One of the most important variance reduction techniques is *importance sampling*. This technique is especially useful for the estimation of very small probabilities. The standard setting is the estimation of a quantity

$$\mu = \mathbb{E}_f H(\boldsymbol{X}) = \int H(\boldsymbol{x})\, f(\boldsymbol{x})\, \mathrm{d}\boldsymbol{x}, \tag{3.17}$$

where H is a real-valued function and f the probability density of a random vector $\boldsymbol{X}$, called the *nominal pdf*. The subscript f is added to the expectation operator to indicate that it is taken with respect to the density f.

NOMINAL PDF

Let g be another probability density such that $g(\boldsymbol{x}) = 0$ implies that $H(\boldsymbol{x})\, f(\boldsymbol{x}) = 0$. Using the density g we can represent μ as

$$\mu = \int H(\boldsymbol{x}) \frac{f(\boldsymbol{x})}{g(\boldsymbol{x})}\, g(\boldsymbol{x})\, \mathrm{d}\boldsymbol{x} = \mathbb{E}_g \left[H(\boldsymbol{X}) \frac{f(\boldsymbol{X})}{g(\boldsymbol{X})} \right]. \tag{3.18}$$

Consequently, if $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N \sim_{\text{iid}} g$, then

$$\widehat{\mu} = \frac{1}{N} \sum_{k=1}^{N} H(\boldsymbol{X}_k) \frac{f(\boldsymbol{X}_k)}{g(\boldsymbol{X}_k)} \tag{3.19}$$

is an unbiased estimator of μ. This estimator is called the *importance sampling estimator* and g is called the importance sampling density. The ratio of densities, $f(\boldsymbol{x})/g(\boldsymbol{x})$, is called the *likelihood ratio*. The importance sampling pseudo-code is given in Algorithm 3.3.2.

IMPORTANCE SAMPLING ESTIMATOR

LIKELIHOOD RATIO

Algorithm 3.3.2: Importance Sampling Estimation

input: Function H, importance sampling density g such that $g(\boldsymbol{x}) = 0$ for all $\boldsymbol{x}$ for which $H(\boldsymbol{x})f(\boldsymbol{x}) = 0$, sample size N, confidence level $1-\alpha$.

output: Point estimate and approximate $(1-\alpha)$ confidence interval for $\mu = \mathbb{E}H(\boldsymbol{X})$, where $\boldsymbol{X} \sim f$.

1 Simulate $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N \overset{\text{iid}}{\sim} g$ and let $Y_i = H(\boldsymbol{X}_i)f(\boldsymbol{X}_i)/g(\boldsymbol{X}_i)$, $i = 1, \ldots, N$.

2 Estimate μ via $\widehat{\mu} = \overline{Y}$ and determine an approximate $(1-\alpha)$ confidence interval as

$$\mathcal{I} := \left(\widehat{\mu} - z_{1-\alpha/2} \frac{S}{\sqrt{N}}, \widehat{\mu} + z_{1-\alpha/2} \frac{S}{\sqrt{N}} \right),$$

where z_γ denotes the γ-quantile of the $\mathcal{N}(0,1)$ distribution and S is the sample standard deviation of $Y_1, \ldots, Y_N$.

3 **return** $\widehat{\mu}$ and the interval $\mathcal{I}$.

■ **Example 3.14 (Importance Sampling)** Let us examine the workings of importance sampling by estimating the area, μ say, under the graph of the function

$$M(x_1, x_2) = \mathrm{e}^{-\frac{1}{4}\sqrt{x_1^2+x_2^2}} \left(\sin\left(2\sqrt{x_1^2 + x_2^2} \right) + 1 \right), \quad (x_1, x_2) \in \mathbb{R}^2. \tag{3.20}$$

☞ 80

We saw a similar function in Example 3.8 (but note the different domain). A natural approach to estimate the area is to truncate the domain to the square $[-b, b]^2$, for large enough b, and to estimate the integral

$$\mu_b = \int_{-b}^{b} \int_{-b}^{b} \underbrace{(2b)^2 M(\boldsymbol{x})}_{H(\boldsymbol{x})} f(\boldsymbol{x}) \, \mathrm{d}\boldsymbol{x} = \mathbb{E}_f H(\boldsymbol{X})$$

via crude Monte Carlo, where $f(\boldsymbol{x}) = 1/(2b)^2, \boldsymbol{x} \in [-b, b]^2$, is the pdf of the uniform distribution on $[-b, b]^2$. Here is the Python code which does just that.

impsamp1.py

```
import numpy as np
from numpy import exp, sqrt, sin, pi, log, cos
from numpy.random import rand

b = 1000
H = lambda x1, x2: (2*b)**2 * exp(-sqrt(x1**2+x2**2)/4)*(sin(2*sqrt(
        x1**2+x2**2))+1)*(x1**2 + x2**2 < b**2)
f = 1/((2*b)**2)
N = 10**6
X1 = -b + 2*b*rand(N,1)
X2 = -b + 2*b*rand(N,1)
Z = H(X1,X2)
estCMC = np.mean(Z).item()  # to obtain scalar
RECMC = np.std(Z)/estCMC/sqrt(N).item()
print('CI = ({:3.3f},{:3.3f}), RE = {: 3.3f}'.format(estCMC*(1-1.96*
    RECMC), estCMC*(1+1.96*RECMC),RECMC))
```

```
CI = (82.663,135.036), RE =  0.123
```

For a truncation level of $b = 1000$ and a sample size of $N = 10^6$, a typical estimate is 108.8, with an estimated relative error of 0.123. We have two sources of error here. The first is the error in approximating μ by μ_b. However, as the function H decays exponentially fast, $b = 1000$ is more than enough to ensure this error is negligible. The second type of error is the statistical error, due to the estimation process itself. This can be quantified by the estimated relative error, and can be reduced by increasing the sample size.

Let us now consider an importance sampling approach in which the importance sampling pdf g is radially symmetric and decays exponentially in the radius, similar to the function H. In particular, we simulate (X_1, X_2) in a way akin to Example 3.1, by first generating a radius $R \sim \mathsf{Exp}(\lambda)$ and an angle $\Theta \sim \mathcal{U}(0, 2\pi)$, and then returning $X_1 = R\cos(\Theta)$ and $X_2 = R\sin(\Theta)$. By the Transformation Rule (Theorem C.4) we then have

☞ 69

☞ 435

$$g(\boldsymbol{x}) = f_{R,\Theta}(r,\theta)\frac{1}{r} = \lambda\,\mathrm{e}^{-\lambda r}\frac{1}{2\pi}\frac{1}{r} = \frac{\lambda \mathrm{e}^{-\lambda\sqrt{x_1^2+x_2^2}}}{2\pi\sqrt{x_1^2+x_2^2}}, \quad \boldsymbol{x} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}.$$

The following code, which imports the one given above, implements the importance sampling steps, using the parameter $\lambda = 0.1$.

impsamp2.py

```
from impsamp1 import *

lam = 0.1;
g = lambda x1, x2: lam*exp(-sqrt(x1**2 + x2**2)*lam)/sqrt(x1**2 + x2
    **2)/(2*pi);
U = rand(N,1); V = rand(N,1)
R = -log(U)/lam
X1 = R*cos(2*pi*V)
X2 = R*sin(2*pi*V)
Z = H(X1,X2)*f/g(X1,X2)
estIS = np.mean(Z).item()  # obtain scalar
REIS = np.std(Z)/estIS/sqrt(N).item()
print('CI = ({:3.3f},{:3.3f}), RE = {: 3.3f}'.format(estIS*(1-1.96*
    REIS), estIS*(1+1.96*REIS),REIS))
```

```
CI = (100.723,101.077), RE =  0.001
```

A typical estimate is 100.90 with an estimated relative error of $1 \cdot 10^{-4}$, which gives a substantial variance reduction. In terms of approximate 95% confidence intervals, we have (82.7,135.0) in the CMC case versus (100.7,101.1) in the importance sampling case. Of course, we could have reduced the truncation level b to improve the performance of CMC, but then the approximation error might become more significant. For the importance sampling case, the relative error is hardly affected by the threshold level, but does depend on the choice of λ. We chose λ such that the decay rate is slower than the decay rate of the function H, which is 0.25. ■

As illustrated in the above example, a main difficulty in importance sampling is how to choose the importance sampling distribution. A poor choice of g may seriously affect the accuracy of both the estimate and the confidence interval. The theoretically optimal choice

g^* for the importance sampling density minimizes the variance of $\widehat{\mu}$ and is therefore the solution to the functional minimization program

$$\min_g \mathbb{V}\mathrm{ar}_g \left(H(\boldsymbol{X}) \frac{f(\boldsymbol{X})}{g(\boldsymbol{X})} \right). \tag{3.21}$$

☞ 118

OPTIMAL IMPORTANCE SAMPLING PDF

It is not difficult to show, see also Exercise 22, that if either $H(\boldsymbol{x}) \geqslant 0$ or $H(\boldsymbol{x}) \leqslant 0$ for all $\boldsymbol{x}$, then the *optimal importance sampling pdf* is

$$g^*(\boldsymbol{x}) = \frac{H(\boldsymbol{x})\, f(\boldsymbol{x})}{\mu}. \tag{3.22}$$

Namely, in this case $\mathbb{V}\mathrm{ar}_{g^*} \widehat{\mu} = \mathbb{V}\mathrm{ar}_{g^*}(H(\boldsymbol{X}) f(\boldsymbol{X})/g(\boldsymbol{X})) = \mathbb{V}\mathrm{ar}_{g^*} \mu = 0$, so that the estimator $\widehat{\mu}$ is *constant* under g^*. An obvious difficulty is that the evaluation of the optimal importance sampling density g^* is usually not possible, since $g^*(\boldsymbol{x})$ in (3.22) depends on the unknown quantity μ. Nevertheless, one can typically choose a good importance sampling density g "close" to the minimum variance density g^*.

One of the main considerations for choosing a good importance sampling pdf is that the estimator (3.19) should have finite variance. This is equivalent to the requirement that

$$\mathbb{E}_g \left[H^2(\boldsymbol{X}) \frac{f^2(\boldsymbol{X})}{g^2(\boldsymbol{X})} \right] = \mathbb{E}_f \left[H^2(\boldsymbol{X}) \frac{f(\boldsymbol{X})}{g(\boldsymbol{X})} \right] < \infty. \tag{3.23}$$

This suggests that g should not have lighter tails than f and that, preferably, the likelihood ratio, f/g, should be bounded.

3.4 Monte Carlo for Optimization

In this section we describe several Monte Carlo methods for optimization. Such randomized algorithms can be useful for solving optimization problems with many local optima and complicated constraints, possibly involving a mix of continuous and discrete variables. Randomized algorithms are also used to solve *noisy* optimization problems, in which the objective function is unknown and has to be obtained via Monte Carlo simulation.

3.4.1 Simulated Annealing

SIMULATED ANNEALING

Simulated annealing is a Monte Carlo technique for minimization that emulates the physical state of atoms in a metal when the metal is heated up and then slowly cooled down. When the cooling is performed very slowly, the atoms settle down to a minimum-energy state. Denoting the state as $\boldsymbol{x}$ and the energy of a state as $S(\boldsymbol{x})$, the probability distribution of the (random) states is described by the *Boltzmann pdf*

$$f(\boldsymbol{x}) \propto \mathrm{e}^{-\frac{S(\boldsymbol{x})}{kT}}, \quad \boldsymbol{x} \in \mathcal{X},$$

where k is Boltzmann's constant and T is the temperature.

Going beyond the physical interpretation, suppose that $S(\boldsymbol{x})$ is an arbitrary function to be minimized, with $\boldsymbol{x}$ taking values in some discrete or continuous set $\mathcal{X}$. The *Gibbs pdf* corresponding to $S(\boldsymbol{x})$ is defined as

GIBBS PDF

$$f_T(\boldsymbol{x}) = \frac{\mathrm{e}^{-\frac{S(\boldsymbol{x})}{T}}}{z_T}, \quad \boldsymbol{x} \in \mathcal{X},$$

provided that the normalization constant $z_T := \sum_{\boldsymbol{x}} \exp(-S(\boldsymbol{x})/T)$ is finite. Note that this is simply the Boltzmann pdf with the Boltzmann constant k removed. As $T \to 0$, the pdf becomes more and more peaked around the set of global minimizers of S.

The idea of simulated annealing is to create a sequence of points $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots$ that are approximately distributed according to pdfs $f_{T_1}(\boldsymbol{x}), f_{T_2}(\boldsymbol{x}), \ldots$, where $T_1, T_2, \ldots$ is a sequence of "temperatures" that decreases (is "cooled") to 0 — known as the *annealing schedule*. If each $\boldsymbol{X}_t$ were sampled *exactly* from f_{T_t}, then $\boldsymbol{X}_t$ would converge to a global minimum of $S(\boldsymbol{x})$ as $T_t \to 0$. However, in practice sampling is *approximate* and convergence to a global minimum is not assured. A generic simulated annealing algorithm is as follows.

ANNEALING SCHEDULE

Algorithm 3.4.1: Simulated Annealing

input: Annealing schedule $T_0, T_1, \ldots,$, function S, initial value $\boldsymbol{x}_0$.
output: Approximations to the global minimizer $\boldsymbol{x}^*$ and minimum value $S(\boldsymbol{x}^*)$.

```
Set X_0 ← x_0 and t ← 1.
while not stopping do
    Approximately simulate X_t from f_{T_t}(x).
    t ← t + 1
return X_t, S(X_t)
```

A popular annealing schedule is *geometric cooling*, where $T_t = \beta T_{t-1}$, $t = 1, 2, \ldots$, for a given initial temperature T_0 and a *cooling factor* $\beta \in (0, 1)$. Appropriate values for T_0 and β are problem-dependent and this has traditionally required tuning on the part of the user. A possible stopping criterion is to stop after a fixed number of iterations, or when the temperature is "small enough".

GEOMETRIC COOLING
COOLING FACTOR

Approximate sampling from a Gibbs distribution is most often carried out via Markov chain Monte Carlo. For each iteration t, the Markov chain should theoretically run for a large number of steps to accurately sample from the Gibbs pdf f_{T_t}. However, in practice, one often only runs a *single* step of the Markov chain, before updating the temperature, as in Algorithm 3.4.2 below.

To sample from a Gibbs distribution f_T, this algorithm uses a random walk Metropolis–Hastings sampler. From (3.7), the acceptance probability of a proposal $\boldsymbol{y}$ is thus

☞ 80

$$\alpha(\boldsymbol{x}, \boldsymbol{y}) = \min\left\{\frac{\mathrm{e}^{-\frac{1}{T}S(\boldsymbol{y})}}{\mathrm{e}^{-\frac{1}{T}S(\boldsymbol{x})}},\ 1\right\} = \min\left\{\mathrm{e}^{-\frac{1}{T}(S(\boldsymbol{y})-S(\boldsymbol{x}))},\ 1\right\}.$$

Hence, if $S(\boldsymbol{y}) < S(\boldsymbol{x})$, then the proposal is aways accepted. Otherwise, the proposal is accepted with probability $\exp(-\frac{1}{T}(S(\boldsymbol{y}) - S(\boldsymbol{x})))$.

Algorithm 3.4.2: Simulated Annealing with a Random Walk Sampler

input: Objective function S, starting state $\boldsymbol{X}_0$, initial temperature T_0, number of iterations N, symmetric proposal density $q(\boldsymbol{y} \mid \boldsymbol{x})$, constant β.
output: Approximate minimizer and minimum value of S.

for $t = 0$ **to** $N - 1$ **do**
  Simulate a new state $\boldsymbol{Y}$ from the symmetric proposal $q(\boldsymbol{y} \mid \boldsymbol{X}_t)$.
  if $S(\boldsymbol{Y}) < S(\boldsymbol{X}_t)$ **then**
    $\boldsymbol{X}_{t+1} \leftarrow \boldsymbol{Y}$
  else
    Draw $U \sim \mathcal{U}(0,1)$.
    if $U \leqslant \mathrm{e}^{-(S(\boldsymbol{Y})-S(\boldsymbol{X}_t))/T_t}$ **then**
      $\boldsymbol{X}_{t+1} \leftarrow \boldsymbol{Y}$
    else
      $\boldsymbol{X}_{t+1} \leftarrow \boldsymbol{X}_t$
  $T_{t+1} \leftarrow \beta T_t$
return $\boldsymbol{X}_N$ and $S(\boldsymbol{X}_N)$

■ **Example 3.15 (Simulated Annealing for Minimization)** Let us minimize the "wiggly" function depicted in the bottom panel of Figure 3.10 and given by:

$$S(x) = \begin{cases} -\mathrm{e}^{-x^2/100} \sin(13x - x^4)^5 \sin(1 - 3x^2)^2, & \text{if } -2 \leqslant x \leqslant 2, \\ \infty, & \text{otherwise.} \end{cases}$$

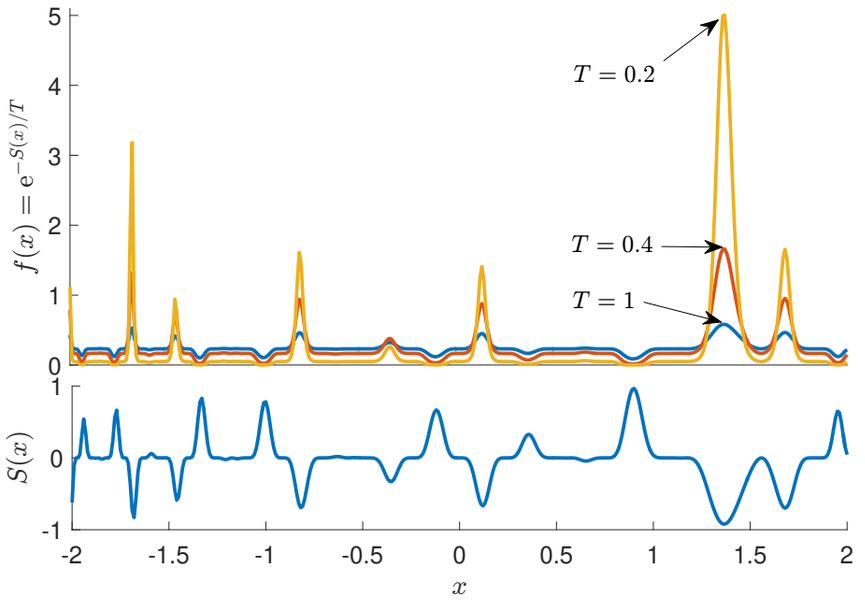


Figure 3.10: Lower panel: the "wiggly" function $S(x)$. Upper panel: three (normalized) Gibbs pdfs for temperatures $T = 1, 0.4, 0.2$. As the temperature decreases, the Gibbs pdf converges to the pdf that has all its mass concentrated at the minimizer of S.

The function has many local minima and maxima, with a global minimum around 1.4. The figure also illustrates the relationship between S and the (unnormalized) Gibbs pdf f_T.

The following Python code implements a slight variant of Algorithm 3.4.2 where, instead of stopping after a fixed number of iterations, the algorithm stops when the temperature is lower than some threshold (here 10^{-3}).

Instead of stopping after a fixed number N of iterations or when the temperature is low enough, it is useful to stop when consecutive function values are closer than some distance ε to each other, or when the best found function value has not changed over a fixed number d of iterations.

For a "current" state x, the proposal state Y is here drawn from the $\mathcal{N}(x, 0.5^2)$ distribution. We use geometric cooling with decay parameter $\beta = 0.999$ and initial temperature $T_0 = 1$. We set the initial state to $x_0 = 0$. Figure 3.11 depicts a realization of the sequence of states x_t for $t = 0, 1, \ldots$. After initially fluctuating wildly, the sequence settles down to a value around 1.37, with $S(1.37) = -0.92$, corresponding to the global optimizer and minimum, respectively.

simann.py

```
import numpy as np
import matplotlib.pyplot as plt

def wiggly(x):
    y = -np.exp(x**2/100)*np.sin(13*x-x**4)**5*np.sin(1-3*x**2)**2
    ind = np.vstack((np.argwhere(x<-2),np.argwhere(x>2)))
    y[ind]=float('inf')
    return y

S = wiggly
beta = 0.999
sig = 0.5
T=1
x= np.array([0])
xx=[]
Sx=S(x)
while T>10**(-3):
    T=beta*T
    y = x+sig*np.random.randn()
    Sy = S(y)
    alpha = np.amin((np.exp(-(Sy-Sx)/T),1))
    if np.random.uniform()<alpha:
        x=y
        Sx=Sy
    xx=np.hstack((xx,x))

print('minimizer = {:3.3f}, minimum ={:3.3f}'.format(x[0],Sx[0]))
plt.plot(xx)
plt.show()
```

```
minimizer = 1.365, minimum = -0.958
```

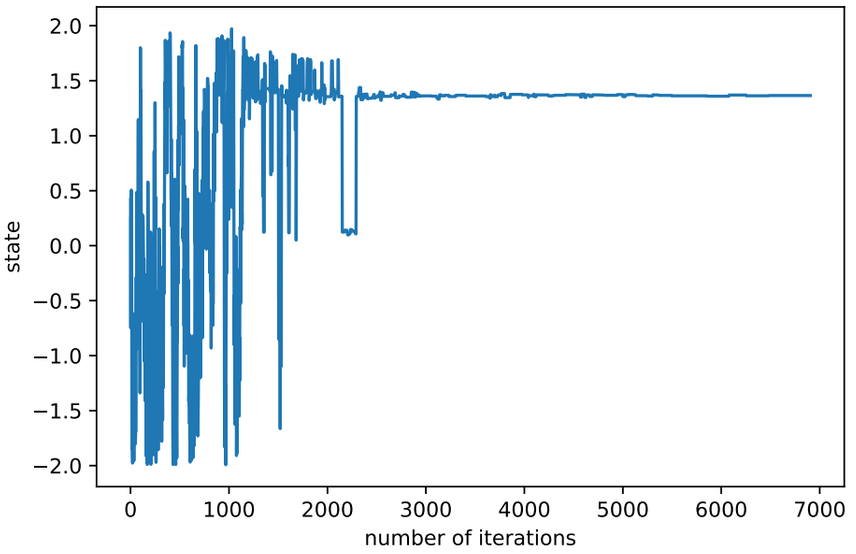


Figure 3.11: Typical states generated by the simulated annealing algorithm.

■

3.4.2 Cross-Entropy Method

CROSS-ENTROPY

The *cross-entropy* (CE) method [103] is a simple Monte Carlo algorithm that can be used for both optimization and estimation.

The basic idea of the CE method for minimizing a function S on a set $\mathcal{X}$ is to define a parametric family of probability densities $\{f(\cdot\,|\,\boldsymbol{v}), \boldsymbol{v} \in \mathcal{V}\}$ on $\mathcal{X}$ and to iteratively update the parameter $\boldsymbol{v}$ so that $f(\cdot\,|\,\boldsymbol{v})$ places more mass on states $\boldsymbol{x}$ that have smaller S values than on the previous iteration. In particular, the CE algorithm has two basic phases:

- *Sampling*: Samples $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$ are drawn independently according to $f(\cdot\,|\,\boldsymbol{v})$. The objective function S is evaluated at these points.
- *Updating*: A new parameter $\boldsymbol{v}'$ is selected on the basis of those $\boldsymbol{X}_i$ for which $S(\boldsymbol{X}_i) \leqslant \gamma$ for some level γ. These $\{\boldsymbol{X}_i\}$ form the *elite sample* set, $\mathcal{E}$.

ELITE SAMPLE

At each iteration the level parameter γ is chosen as the worst of the $N^{\text{elite}} := \lceil \varrho N \rceil$ best performing samples, where $\varrho \in (0,1)$ is the *rarity parameter* — typically, $\varrho = 0.1$ or $\varrho = 0.01$. The parameter $\boldsymbol{v}$ is updated as a smoothed average $\alpha \boldsymbol{v}' + (1-\alpha)\boldsymbol{v}$, where $\alpha \in (0,1)$ is the *smoothing parameter* and

RARITY PARAMETER

SMOOTHING PARAMETER

$$\boldsymbol{v}' := \operatorname*{argmax}_{\boldsymbol{v} \in \mathcal{V}} \sum_{\boldsymbol{X} \in \mathcal{E}} \ln f(\boldsymbol{X}\,|\,\boldsymbol{v}). \tag{3.24}$$

The updating rule (3.24) is the result of minimizing the Kullback–Leibler divergence between the conditional density of $\boldsymbol{X} \sim f(\boldsymbol{x}\,|\,\boldsymbol{v})$ given $S(\boldsymbol{X}) \leqslant \gamma$, and $f(\boldsymbol{x}; \boldsymbol{v})$; see [103]. Note that (3.24) yields the *maximum likelihood estimator* (MLE) of $\boldsymbol{v}$ based on the elite samples. Hence, for many specific families of distributions, explicit solutions can be found. An important example is where $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \operatorname{diag}(\boldsymbol{\sigma}^2))$; that is, $\boldsymbol{X}$ has independent Gaussian

☞ 458

components. In this case, the mean vector $\boldsymbol{\mu}$ and the vector of variances $\boldsymbol{\sigma}^2$ are simply updated via the sample mean and sample variance of the elite samples. This is known as *normal updating*. A generic CE procedure for minimization is given in Algorithm 3.4.3.

NORMAL UPDATING

Algorithm 3.4.3: Cross-Entropy Method for Minimization

input: Function S, initial sampling parameter $\boldsymbol{v}_0$, sample size N, rarity parameter ϱ, smoothing parameter α.

output: Approximate minimum of S and optimal sampling parameter $\boldsymbol{v}$.

1 Initialize $\boldsymbol{v}_0$, set $N^{\text{elite}} \leftarrow \lceil \varrho N \rceil$ and $t \leftarrow 0$.

2 **while** a stopping criterion is not met **do**

3 $\quad t \leftarrow t + 1$

4 $\quad$ Simulate an iid sample $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$ from the density $f(\cdot \,|\, \boldsymbol{v}_{t-1})$.

5 $\quad$ Evaluate the performances $S(\boldsymbol{X}_1), \ldots, S(\boldsymbol{X}_N)$ and sort them from smallest to largest: $S_{(1)}, \ldots, S_{(N)}$.

6 $\quad$ Let γ_t be the sample ϱ-quantile of the performances:

$$\gamma_t \leftarrow S_{(N^{\text{elite}})}. \tag{3.25}$$

7 $\quad$ Determine the set of elite samples $\mathcal{E}_t = \{\boldsymbol{X}_i : S(\boldsymbol{X}_i) \leqslant \gamma_t\}$.

8 $\quad$ Let $\boldsymbol{v}'_t$ be the MLE of the elite samples:

$$\boldsymbol{v}'_t \leftarrow \operatorname*{argmax}_{\boldsymbol{v}} \sum_{\boldsymbol{X} \in \mathcal{E}_t} \ln f(\boldsymbol{X} \,|\, \boldsymbol{v}). \tag{3.26}$$

9 $\quad$ Update the sampling parameter as

$$\boldsymbol{v}_t \leftarrow \alpha \boldsymbol{v}'_t + (1 - \alpha) \boldsymbol{v}_{t-1}. \tag{3.27}$$

10 **return** γ_t, $\boldsymbol{v}_t$

The CE algorithm produces a sequence of pairs $(\gamma_1, \boldsymbol{v}_1), (\gamma_2, \boldsymbol{v}_2), \ldots$, such that γ_t converges (approximately) to the minimal function value, and $f(\cdot \,|\, \boldsymbol{v}_t)$ to a degenerate pdf that (approximately) concentrates all its mass at a minimizer of S, as $t \to \infty$. A possible stopping condition is to stop when the sampling distribution $f(\cdot \,|\, \boldsymbol{v}_t)$ is sufficiently close to a degenerate distribution. For normal updating this means that the standard deviation is sufficiently small.

The output of the CE algorithm could also include the overall best function value and corresponding solution.

In the following example, we minimize the same function as in Example 3.15, but instead use the CE algorithm. ☞ 97

■ **Example 3.16 (Cross-Entropy Method for Minimization)** In this case we take the family of normal distributions $\{\mathcal{N}(\mu, \sigma^2)\}$ for the sampling step (Step 4 of Algorithm 3.4.3), starting with $\mu = 0$ and $\sigma = 3$. The choice of the initial parameter is quite arbitrary, as long as σ is large enough to sample a wide range of points. We take $N = 100$ samples at each iteration, set $\varrho = 0.1$, and keep the $N^{\text{elite}} = 10 = \lceil N\varrho \rceil$ smallest ones as the elite samples. The parameters μ and σ are then updated via the sample mean and sample standard deviation

of the elite samples. In this case we do not use any smoothing ($\alpha = 1$). In the following Python code the 100×2 matrix `Sx` stores the x-values in the first column and the function values in the second column. The rows of this matrix are sorted in ascending order according to the function values, giving the matrix `sortSx`. The first $N^{\text{elite}} = 10$ rows of this sorted matrix correspond to the elite samples and their function values. The updating of μ and σ is done in Lines 14 and 15. Figure 3.12 shows how the pdfs of the $\mathcal{N}(\mu_t, \sigma_t^2)$ sampling distributions degenerate to the point mass at the global minimizer 1.366.

CEmethod.py

```
from simann import wiggly
import numpy as np
np.set_printoptions(precision=3)
mu, sigma = 0, 3
N, Nel = 100, 10
eps = 10**-5
S = wiggly
while sigma > eps:
    X = np.random.randn(N,1)*sigma + np.array(np.ones((N,1)))*mu
    Sx = np.hstack((X, S(X)))
    sortSx = Sx[Sx[:,1].argsort(),]
    Elite = sortSx[0:Nel,:-1]
    mu = np.mean(Elite, axis=0)
    sigma = np.std(Elite, axis=0)
    print('S(mu)= {}, mu: {}, sigma: {}\n'.format(S(mu), mu, sigma))
```

```
S(mu)= [0.071], mu: [0.414], sigma: [0.922]
S(mu)= [0.063], mu: [0.81], sigma: [0.831]
S(mu)= [-0.033], mu: [1.212], sigma: [0.69]
S(mu)= [-0.588], mu: [1.447], sigma: [0.117]
S(mu)= [-0.958], mu: [1.366], sigma: [0.007]
S(mu)= [-0.958], mu: [1.366], sigma: [0.]
S(mu)= [-0.958], mu: [1.366], sigma: [3.535e-05]
S(mu)= [-0.958], mu: [1.366], sigma: [2.023e-06]
```

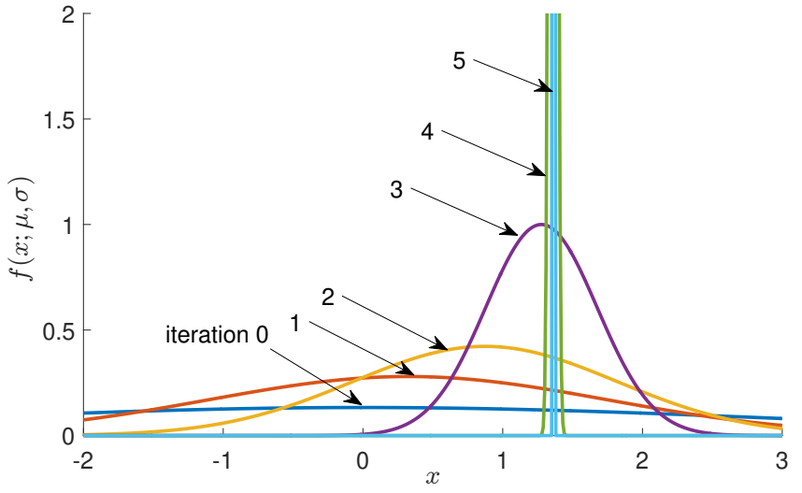


Figure 3.12: The normal pdfs of the first six sampling distributions, truncated to the interval $[-2, 3]$. The initial sampling distribution is $\mathcal{N}(0, 3^2)$.

3.4.3 Splitting for Optimization

Minimizing a function $S(\boldsymbol{x})$, $\boldsymbol{x} \in \mathcal{X}$ is closely related to drawing a random sample from a *level set* of the form $\{\boldsymbol{x} \in \mathcal{X} : S(\boldsymbol{x}) \leqslant \gamma\}$. Suppose S has minimum value γ^* attained at $\boldsymbol{x}^*$. As long as $\gamma \geqslant \gamma^*$, this level set contains the minimizer. Moreover, if γ is close to γ^*, the volume of this level set will be small. So, a randomly selected point from this set is expected to be close to $\boldsymbol{x}^*$. Thus, by gradually decreasing the level parameter γ, the level sets will gradually shrink towards the set $\{\boldsymbol{x}^*\}$. Indeed, the CE method was developed with exactly this connection in mind; see, e.g., [102]. Note that the CE method employs a *parametric* sampling distribution to obtain samples from the level sets (the elite samples). In [34] a *non-parametric* sampling mechanism is introduced that uses an evolving collection of particles. The resulting optimization algorithm, called *splitting for continuous optimization* (SCO), provides a fast and accurate way to optimize complicated continuous functions. The details of SCO are given in Algorithm 3.4.4.

LEVEL SET

SPLITTING FOR CONTINUOUS OPTIMIZATION

Algorithm 3.4.4: Splitting for Continuous Optimization (SCO)

input: Objective function S, sample size N, rarity parameter ϱ, scale factor w, bounded region $\mathcal{B} \subset \mathcal{X}$ that is known to contain a global minimizer, and maximum number of attempts `MaxTry`.

output: Final iteration number t and sequence $(\boldsymbol{X}_{\text{best},1}, b_1), \ldots, (\boldsymbol{X}_{\text{best},t}, b_t)$ of best solutions and function values at each iteration.

Simulate $\mathcal{Y}_0 = \{\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_N\}$ uniformly on $\mathcal{B}$. Set $t \leftarrow 0$ and $N^{\text{elite}} \leftarrow \lceil N\varrho \rceil$.
while stopping condition is not satisfied **do**
  Determine the N^{elite} smallest values, $S_{(1)} \leqslant \cdots \leqslant S_{(N^{\text{elite}})}$, of $\{S(\boldsymbol{X}), \boldsymbol{X} \in \mathcal{Y}_t\}$, and store the corresponding vectors, $\boldsymbol{X}_{(1)}, \ldots, \boldsymbol{X}_{(N^{\text{elite}})}$, in $\mathcal{X}_{t+1}$. Set $b_{t+1} \leftarrow S_{(1)}$ and $\boldsymbol{X}_{\text{best},t+1} \leftarrow \boldsymbol{X}_{(1)}$.
  Draw $B_i \sim \text{Bernoulli}(\frac{1}{2})$, $i = 1, \ldots, N^{\text{elite}}$, with $\sum_{i=1}^{N^{\text{elite}}} B_i = N \bmod N^{\text{elite}}$.
  for $i = 1$ **to** N^{elite} **do**
    $R_i \leftarrow \left\lfloor \frac{N}{N^{\text{elite}}} \right\rfloor + B_i$ `// random splitting factor`
    $\boldsymbol{Y} \leftarrow \boldsymbol{X}_{(i)}$; $\boldsymbol{Y}' \leftarrow \boldsymbol{Y}$
    for $j = 1$ **to** R_i **do**
      Draw $I \in \{1, \ldots, N^{\text{elite}}\} \setminus \{i\}$ uniformly and let $\boldsymbol{\sigma}_i \leftarrow w|\boldsymbol{X}^{(i)} - \boldsymbol{X}^{(I)}|$.
      Simulate a uniform permutation $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_n)$ of $(1, \ldots, n)$.
      for $k = 1$ **to** n **do**
        for `Try` $= 1$ **to** `MaxTry` **do**
          $\boldsymbol{Y}'(\pi_k) \leftarrow \boldsymbol{Y}(\pi_k) + \boldsymbol{\sigma}_i(\pi_k) Z, \quad Z \sim \mathcal{N}(0,1)$
          if $S(\boldsymbol{Y}') < S(\boldsymbol{Y})$ **then** $\boldsymbol{Y} \leftarrow \boldsymbol{Y}'$ and **break**.
      Add $\boldsymbol{Y}$ to $\mathcal{Y}_{t+1}$
  $t \leftarrow t + 1$
return $\{(\boldsymbol{X}_{\text{best},k}, b_k), k = 1, \ldots, t\}$

At iteration $t = 0$, the algorithm starts with a population of particles $\mathcal{Y}_0 = \{\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_N\}$ that are uniformly generated on some bounded region $\mathcal{B}$, which is large enough to contain a global minimizer. The function values of all particles in $\mathcal{Y}_0$ are sorted, and the best

$N^{\text{elite}} = \lceil N\varrho \rceil$ form the elite particle set $\mathcal{X}_1$, exactly as in the CE method. Next, the elite particles are "split" into $\lfloor N/N^{\text{elite}} \rfloor$ children particles, adding one extra child to some of the elite particles to ensure that the total number of children is again N. The purpose of Line 4 is to randomize which elite particles receive an extra child. Lines 8–15 describe how the children of the i-th elite particle are generated. First, in Line 9, we select one of the *other* elite particles uniformly at random. The same line defines an n-dimensional vector $\boldsymbol{\sigma}_i$ whose components are the absolute differences between the vectors $\boldsymbol{X}_{(i)}$ and $\boldsymbol{X}_{(I)}$, multiplied by a constant w. That is,

$$\boldsymbol{\sigma}_i = w\,|\boldsymbol{X}_{(i)} - \boldsymbol{X}_{(I)}| := w \begin{bmatrix} |X_{(i),1} - X_{(I),1}| \\ |X_{(i),2} - X_{(I),2}| \\ \vdots \\ |X_{(i),n} - X_{(I),n}| \end{bmatrix}.$$

☞ 115

Next, a uniform random permutation $\boldsymbol{\pi}$ of $(1, \ldots, n)$ is simulated (see Exercise 9). Lines 11–14 describe how, starting from a candidate child point $\boldsymbol{Y}$, each coordinate of $\boldsymbol{Y}$ is resampled, in the order determined by $\boldsymbol{\pi}$, by adding a standard normal random variable to that component, multiplied by the corresponding component of $\boldsymbol{\sigma}_i$ (Line 13). If the resulting $\boldsymbol{Y}'$ has a function value that is less than that of $\boldsymbol{Y}$, then the new candidate is accepted. Otherwise, the *same* coordinate is tried again. If no improvement is found in `MaxTry` attempts, the original component is retained. This process is performed for all elite samples, to produce the first-generation population $\mathcal{Y}_1$. The procedure is then repeated for iterations $t = 1, 2, \ldots$, until some stopping criterion is met, e.g., when the best found function value does not change for a number of consecutive iterations, or when the total number of function evaluations exceeds some threshold. The best found function value and corresponding argument (particle) are returned at the conclusion of the algorithm.

The input variable `MaxTry` governs how much computational time is dedicated to updating a component. In most cases we have encountered, the choices $w = 0.5$ and `MaxTry` $= 5$ work well. Empirically, relatively high value for ϱ work well, such as $\varrho = 0.4, 0.8$, or even $\varrho = 1$. The latter case means that at each stage t *all* samples from $\mathcal{Y}_{t-1}$ carry over to the elite set $\mathcal{X}_t$.

■ **Example 3.17 (Test Problem 112)** Hock and Schittkowski [58] provide a rich source of test problems for multiextremal optimization. A challenging one is Problem 112, where the goal is to find $\boldsymbol{x}$ so as to minimize the function

$$S(\boldsymbol{x}) = \sum_{j=1}^{10} x_j \left(c_j + \ln \frac{x_j}{x_1 + \cdots + x_{10}} \right),$$

subject to the following set of constraints:

$$\begin{aligned} x_1 + 2x_2 + 2x_3 + x_6 + x_{10} - 2 &= 0, \\ x_4 + 2x_5 + x_6 + x_7 - 1 &= 0, \\ x_3 + x_7 + x_8 + 2x_9 + x_{10} - 1 &= 0, \\ x_j &\geqslant 0.000001, \quad j = 1, \ldots, 10, \end{aligned}$$

where the constants $\{c_i\}$ are given in Table 3.1.

Table 3.1: Constants for Test Problem 112.

$c_1 = -6.089$	$c_2 = -17.164$	$c_3 = -34.054$	$c_4 = -5.914$	$c_5 = -24.721$
$c_6 = -14.986$	$c_7 = -24.100$	$c_8 = -10.708$	$c_9 = -26.662$	$c_{10} = -22.179$

The best known minimal value in [58] was −47.707579. In [89] a better solution was found, −47.760765, using a genetic algorithm. The corresponding solution vector was completely different from the one in [58]. A further improvement,−47.76109081, was found in [70], using the CE method, giving a similar solution vector to that in [89]:

0.04067247	0.14765159	0.78323637	0.00141368	0.48526222
0.00069291	0.02736897	0.01794290	0.03729653	0.09685870

To obtain a solution with SCO, we first converted this 10-dimensional problem into a 7-dimensional one by defining the objective function

$$S_7(\boldsymbol{y}) = S(\boldsymbol{x}),$$

where $x_2 = y_1, x_3 = y_2, x_5 = y_3, x_6 = y_4, x_7 = y_5, x_9 = y_6, x_{10} = y_7$, and

$$\begin{aligned} x_1 &= 2 - (2y_1 + 2y_2 + y_4 + x_7), \\ x_4 &= 1 - (2y_3 + y_4 + y_5), \\ x_8 &= 1 - (y_2 + y_5 + 2y_6 + y_7), \end{aligned}$$

subject to $x_1, \ldots, x_{10} \geqslant 0.000001$, where the $\{x_i\}$ are taken as functions of the $\{y_i\}$. We then adopted a penalty approach (see Section B.4) by adding a penalty function to the original objective function:

☞ 417

$$\widetilde{S}_7(\boldsymbol{y}) = S(\boldsymbol{x}) + 1000 \sum_{i=1}^{10} \max\{-(x_i - 0.000001), 0\},$$

where, again, the $\{x_i\}$ are defined in terms of the $\{y_i\}$ as above.

Optimizing this last function with SCO, we found, in less time than the other algorithms, a slightly smaller function value: −47.761090859365858, with solution vector

0.040668102417464	0.147730393049955	0.783153291185250	0.001414221643059
0.485246633088859	0.000693172682617	0.027399339496606	0.017947274343948
0.037314369272343	0.096871356429511		

in line with the earlier solutions. ■

3.4.4 Noisy Optimization

In *noisy optimization*, the objective function is unknown, but estimates of function values are available, e.g., via simulation. For example, to find an optimal prediction function g in supervised learning, the exact risk $\ell(g) = \mathbb{E}\,\mathrm{Loss}(Y, g(\boldsymbol{x}))$ is usually unknown and only estimates of the risk are available. Optimizing the risk is thus typically a noisy optimization problem. Noisy optimization features prominently in simulation studies where

NOISY OPTIMIZATION

☞ 20

the behavior of some system (e.g., vehicles on a road network) is simulated under certain parameters (e.g., the lengths of the traffic light intervals) and the aim is to choose those parameters optimally (e.g., to maximize the traffic throughput). For each parameter setting the exact value for the objective function is unknown but estimates can be obtained via the simulation.

In general, suppose the goal is to minimize a function S, where S is unknown, but an estimate of $S(\boldsymbol{x})$ can be obtained for any choice of $\boldsymbol{x} \in \mathcal{X}$. Because the gradient ∇S is unknown, one cannot directly apply classical optimization methods. The *stochastic approximation* method mimics the classical gradient descent method by replacing a deterministic gradient with an estimate $\widehat{\nabla S}(\boldsymbol{x})$.

STOCHASTIC APPROXIMATION

A simple estimator for the i-th component of $\nabla S(\boldsymbol{x})$ (that is, $\partial S(\boldsymbol{u})/\partial x_i$), is the *central difference estimator*

CENTRAL DIFFERENCE ESTIMATOR

$$\frac{\widehat{S}(\boldsymbol{x} + \boldsymbol{e}_i\,\delta/2) - \widehat{S}(\boldsymbol{x} - \boldsymbol{e}_i\,\delta/2)}{\delta}, \tag{3.28}$$

where $\boldsymbol{e}_i$ denotes the i-th unit vector, and $\widehat{S}(\boldsymbol{x}+\boldsymbol{e}_i\,\delta/2)$ and $\widehat{S}(\boldsymbol{x}-\boldsymbol{e}_i\,\delta/2)$ can be any estimators of $S(\boldsymbol{x} + \boldsymbol{e}_i\,\delta/2)$ and $S(\boldsymbol{x} - \boldsymbol{e}_i\,\delta/2)$, respectively. The difference parameter $\delta > 0$ should be small enough to reduce the bias of the estimator, but large enough to keep the variance of the estimator small.

To reduce the variance in the estimator (3.28) it is important to have $\widehat{S}(\boldsymbol{x} + \boldsymbol{e}_i\,\delta/2)$ and $\widehat{S}(\boldsymbol{x} - \boldsymbol{e}_i\,\delta/2)$ positively correlated. This can for example be achieved by using *common random numbers* in the simulation.

COMMON RANDOM NUMBERS

☞ 414

In direct analogy to gradient descent methods, the stochastic approximation method produces a sequence of iterates, starting with some $\boldsymbol{x}_1 \in \mathcal{X}$, via

$$\boldsymbol{x}_{t+1} = \boldsymbol{x}_t - \beta_t\,\widehat{\nabla S}(\boldsymbol{x}_t), \tag{3.29}$$

where $\beta_1, \beta_2, \ldots$ is a sequence of strictly positive step sizes. A generic stochastic approximation algorithm for minimizing a function S is thus as follows.

Algorithm 3.4.5: Stochastic Approximation

input: A mechanism to estimate any gradient $\nabla S(\boldsymbol{x})$ and step sizes $\beta_1, \beta_2, \ldots$.
output: Approximate optimizer of S.

```
Initialize x_1 ∈ X. Set t ← 1.
while a stopping criterion is not met do
    Obtain an estimated gradient ∇̂S(x_t) of S at x_t.
    Determine a step size β_t.
    Set x_{t+1} ← x_t − β_t ∇̂S(x_t).
    t ← t + 1
return x_t
```

When $\widehat{\nabla S}(\boldsymbol{x}_t)$ is an *unbiased* estimator of $\nabla S(\boldsymbol{x}_t)$ in (3.29) the stochastic approximation Algorithm 3.4.5 is referred to as the *Robbins–Monro* algorithm. When finite differences are used to estimate $\widehat{\nabla S}(\boldsymbol{x}_t)$, as in (3.28), the resulting algorithm is known as the

ROBBINS–MONRO

Kiefer–Wolfowitz algorithm. In Section 9.4.1 we will see how stochastic gradient descent is employed in deep learning to minimize the training loss, based on a "minibatch" of training data.

KIEFER–WOLFOWITZ
☞ 336

It can be shown [72] that, under certain regularity conditions on S, the sequence $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$ converges to the true minimizer $\boldsymbol{x}^*$ when the step sizes decrease slowly enough to 0; in particular, when

$$\sum_{t=1}^{\infty} \beta_t = \infty \quad \text{and} \quad \sum_{t=1}^{\infty} \beta_t^2 < \infty. \tag{3.30}$$

In practice, one rarely uses step sizes that satisfy (3.30), as the convergence of the sequence will be too slow to be of practical use.

An alternative approach to stochastic approximation is the *stochastic counterpart* method, also called *sample average approximation*. It can be applied in situations where the noisy objective function is of the form

STOCHASTIC COUNTERPART

$$S(\boldsymbol{x}) = \mathbb{E}\widetilde{S}(\boldsymbol{x}, \boldsymbol{\xi}), \quad \boldsymbol{x} \in \mathcal{X}, \tag{3.31}$$

where $\boldsymbol{\xi}$ is a random vector that can be simulated and $\widetilde{S}(\boldsymbol{x}, \boldsymbol{\xi})$ can be evaluated exactly. The idea is to replace the optimization of (3.31) with that of the sample average

$$\widehat{S}(\boldsymbol{x}) = \frac{1}{N} \sum_{i=1}^{N} \widetilde{S}(\boldsymbol{x}, \boldsymbol{\xi}_i), \quad \boldsymbol{x} \in \mathcal{X}, \tag{3.32}$$

where $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_N$ are iid copies of $\boldsymbol{\xi}$. Note that $\widehat{S}$ is a deterministic function of $\boldsymbol{x}$ and so can be optimized using any optimization algorithm. A solution to this sample average version is taken to be an estimator of a solution $\boldsymbol{x}^*$ to the original problem (3.31).

■ **Example 3.18 (Determining Good Importance Sampling Parameters)** The selection of good importance sampling parameters can be viewed as a stochastic optimization problem. Consider, for instance, the importance sampling estimator in Example 3.14. Recall that the nominal distribution is the uniform distribution on the square $[-b, b]^2$, with pdf

☞ 94

$$f_b(\boldsymbol{x}) = \frac{1}{(2b)^2}, \quad \boldsymbol{x} \in [-b, b]^2,$$

where b is large enough to ensure that μ_b is close to μ; in that example, we chose $b = 1000$. The importance sampling pdf is

$$g_\lambda(\boldsymbol{x}) = f_{R,\Theta}(r, \theta)\frac{1}{r} = \lambda \mathrm{e}^{-\lambda r}\frac{1}{2\pi}\frac{1}{r} = \frac{\lambda \mathrm{e}^{-\lambda\sqrt{x_1^2+x_2^2}}}{2\pi\sqrt{x_1^2+x_2^2}}, \quad \boldsymbol{x} = (x_1, x_2) \in \mathbb{R}^2 \setminus \{\mathbf{0}\},$$

which depends on a free parameter λ. In the example we chose $\lambda = 0.1$. Is this the best choice? Maybe $\lambda = 0.05$ or 0.2 would have resulted in a more accurate estimate. The important thing to realize is that the "effectiveness" of λ can be measured in terms of the variance of the estimator $\widehat{\mu}$ in (3.19), which is given by

☞ 93

$$\frac{1}{N}\mathbb{V}\mathrm{ar}_{g_\lambda}\left(H(\boldsymbol{X})\frac{f(\boldsymbol{X})}{g_\lambda(\boldsymbol{X})}\right) = \frac{1}{N}\mathbb{E}_{g_\lambda}\left[H^2(\boldsymbol{X})\frac{f^2(\boldsymbol{X})}{g_\lambda^2(\boldsymbol{X})}\right] - \frac{\mu^2}{N} = \frac{1}{N}\mathbb{E}_f\left[H^2(\boldsymbol{X})\frac{f(\boldsymbol{X})}{g_\lambda(\boldsymbol{X})}\right] - \frac{\mu^2}{N}.$$

Hence, the optimal parameter λ^* minimizes the function $S(\lambda) = \mathbb{E}_f[H^2(\boldsymbol{X})f(\boldsymbol{X})/g_\lambda(\boldsymbol{X})]$, which is unknown, but can be estimated from simulation. To solve this stochastic minimization problem, we first use stochastic approximation. Thus, at each step of the algorithm, the gradient of $S(\lambda)$ is estimated from realizations of $\widehat{S}(\lambda) = H^2(\boldsymbol{X})f(\boldsymbol{X})/g_\lambda(\boldsymbol{X})$, where $\boldsymbol{X} \sim f_b$. As in the original problem (that is, the estimation of μ), the parameter b should be large enough to avoid any bias in the estimator of λ^*, but also small enough to ensure a small variance. The following Python code implements a particular instance of Algorithm 3.4.5. For sampling from f_b here, we used $b = 100$ instead of $b = 1000$, as this will improve the crude Monte Carlo estimation of λ^*, without noticeably affecting the bias. The gradient of $S(\lambda)$ is estimated in Lines 11–17, using the central difference estimator (3.28). Notice how for the $S(\lambda-\delta/2)$ and $S(\lambda+\delta/2)$ the *same* random vector $\boldsymbol{X} = [X_1, X_2]^\top$ is used.

☞ 118

This significantly reduces the variance of the gradient estimator; see also Exercise 23. The step size β_t should be such that $\beta_t\widehat{\nabla S}(\boldsymbol{x}_t) \approx \lambda_t$. Given the large gradient here, we choose $\beta_0 = 10^{-7}$ and decrease it each step by a factor of 0.99. Figure 3.13 shows how the sequence $\lambda_0, \lambda_1, \ldots$ decreases towards approximately 0.125, which we take as an estimator for the optimal importance sampling parameter λ^*.

stochapprox.py

```
import numpy as np
from numpy import pi
import matplotlib.pyplot as plt

b=100    # choose b large enough, but not too large
delta = 0.01
H = lambda x1, x2: (2*b)**2*np.exp(-np.sqrt(x1**2 + x2**2)/4)*(np.
    sin(2*np.sqrt(x1**2+x2**2)+1))*(x1**2+x2**2<b**2)
f = 1/(2*b)**2
g = lambda x1, x2, lam: lam*np.exp(-np.sqrt(x1**2+x2**2)*lam)/np.
    sqrt(x1**2+x2**2)/(2*pi)
beta = 10**-7   #step size very small, as the gradient is large
lam=0.25
lams = np.array([lam])
N=10**4
for i in range(200):
    x1 = -b + 2*b*np.random.rand(N,1)
    x2 = -b + 2*b*np.random.rand(N,1)
    lamL = lam - delta/2
    lamR = lam + delta/2
    estL = np.mean(H(x1,x2)**2*f/g(x1, x2, lamL))
    estR = np.mean(H(x1,x2)**2*f/g(x1, x2, lamR))  #use SAME x1,x2
    gr = (estR-estL)/delta  #gradient
    lam = lam - gr*beta  #gradient descend
    lams = np.hstack((lams, lam))
    beta = beta*0.99

lamsize=range(0, (lams.size))
plt.plot(lamsize, lams)
plt.show()
```

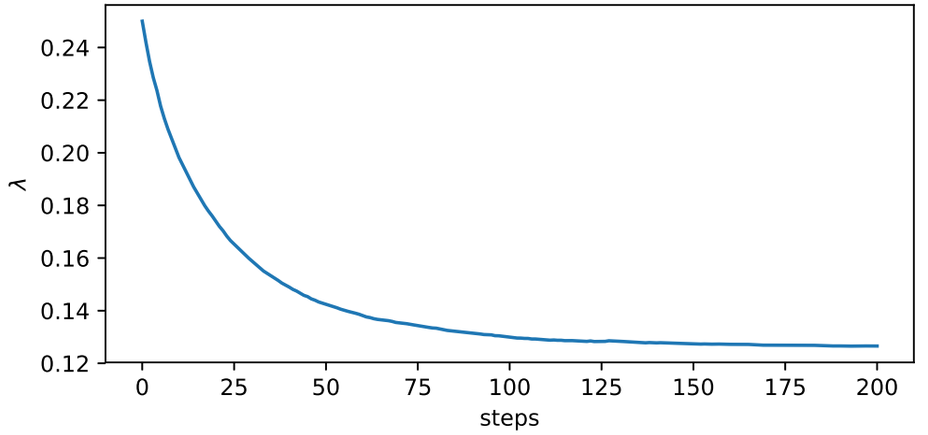


Figure 3.13: The stochastic optimization algorithm produces a sequence $\lambda_t, t = 0, 1, 2, \ldots$ that tends to an approximate estimate of the optimal importance sampling parameter $\lambda^* \approx 0.125$.

Next, we estimate λ^* using a stochastic counterpart approach. As the objective function $S(\lambda)$ is of the form (3.31) (with λ taking the role of $\boldsymbol{x}$ and $\boldsymbol{X}$ the role of $\boldsymbol{\xi}$), we obtain the sample average

$$\widehat{S}(\lambda) = \frac{1}{N} \sum_{i=1}^{N} H^2(\boldsymbol{X}_i) \frac{f(\boldsymbol{X}_i)}{g_\lambda(\boldsymbol{X}_i)}, \tag{3.33}$$

where $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N \sim_{\text{iid}} f_b$. Once the $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N \sim_{\text{iid}} f_b$ have been simulated, $\widehat{S}(\lambda)$ is a deterministic function of λ, which can be optimized by any means. We take the most basic approach and simply evaluate the function for $\lambda = 0.01, 0.02, \ldots, 0.3$ and select the minimizing λ on this grid. The code is given below and Figure 3.14 shows $\widehat{S}(\lambda)$ as a function of λ. The minimum value found was $0.60 \cdot 10^4$ for minimizer $\widehat{\lambda}^* = 0.12$, which is in accordance with the value obtained via stochastic approximation. The sensitivity of this estimate can be assessed from the graph: for a wide range of values (say from 0.04 to 0.15) $\widehat{S}$ stays rather flat. So any of these values could be used in an importance sampling procedure to estimate μ. However, very small values (less than 0.02) and large values (greater than 0.25) should be avoided. Our original choice of $\lambda = 0.1$ was therefore justified and we could not have done much better.

stochcounterpart.py

```
from stochapprox import *

lams = np.linspace(0.01, 0.31, 1000)
res=[]
res = np.array(res)
for i in range(lams.size):
    lam = lams[i]
    np.random.seed(1)
    g = lambda x1, x2: lam*np.exp(-np.sqrt(x1**2+x2**2)*lam)/np.sqrt
        (x1**2+x2**2)/(2*pi)
```

```
    X=-b+2*b*np.random.rand(N,1)
    Y=-b+2*b*np.random.rand(N,1)
    Z=H(X,Y)**2*f/g(X,Y)
    estCMC = np.mean(Z)
    res = np.hstack((res, estCMC))

plt.plot(lams, res)
plt.xlabel(r'$\lambda$')
plt.ylabel(r'$\hat{S}(\lambda)$')
plt.ticklabel_format(style='sci', axis='y', scilimits=(0,0))
plt.show()
```

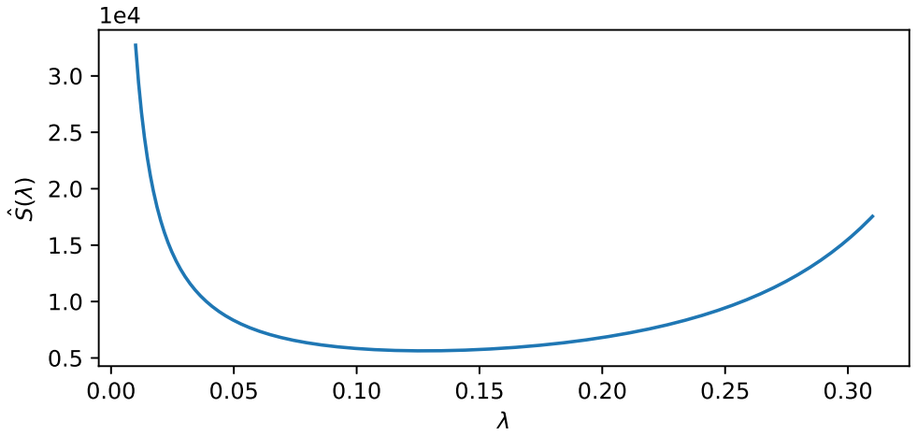


Figure 3.14: The stochastic counterpart method replaces the unknown $S(\lambda)$ (that is, the scaled variance of the importance sampling estimator) with its sample average, $\widehat{S}(\lambda)$. The minimum value of $\widehat{S}$ is attained around $\lambda = 0.12$.

■

A third method for stochastic optimization is the cross-entropy method. In particular, Algorithm 3.4.3 can easily be modified to minimize *noisy* functions $S(\boldsymbol{x}) = \mathbb{E}\widetilde{S}(\boldsymbol{x}, \boldsymbol{\xi})$, as defined in (3.31). The only change required in the algorithm is that every function value $S(\boldsymbol{x})$ be replaced by its estimate $\widehat{S}(\boldsymbol{x})$. Depending on the level of noise in the function, the sample size N might have to be increased considerably.

☞ 101

■ **Example 3.19 (Cross-Entropy Method for Noisy Optimization)** To explore the use of the CE method for noisy optimization, take the following noisy discrete optimization problem. Suppose there is a "black box" that contains an unknown binary sequence of n bits. If one feeds the black box any input vector, it will first scramble the input by independently flipping the bits (changing 0 to 1 and 1 to 0) with a probability θ and then return the number of bits that do not match the true (unknown) binary sequence. This is illustrated in Figure 3.15 for $n = 10$.

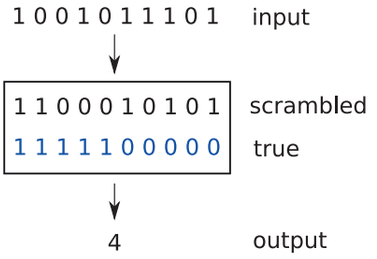


Figure 3.15: A noisy optimization function as a black box. The input to the black box is a binary vector. Inside the black box the digits of the input vector are scrambled by flipping bits with probability θ. The output is the number of bits of the scrambled vector that do not match the true (unknown) binary vector.

Denoting by $S(\boldsymbol{x})$ the true number of matching digits for a binary input vector $\boldsymbol{x}$, the black box thus returns a noisy estimate $\widehat{S}(\boldsymbol{x})$. The objective is to estimate the binary sequence inside the black box, by feeding it with many input vectors and observing their output. Or, to put it in a different way, to minimize $S(\boldsymbol{x})$ using $\widehat{S}(\boldsymbol{x})$ as a proxy. Since there are 2^n possible input vectors, it is infeasible to try all possible vectors $\boldsymbol{x}$ even for moderate n.

The following Python program implements the noisy function $\widehat{S}(\boldsymbol{x})$ for $n = 100$. Each input bit is flipped with a rather high probability $\theta = 0.4$, so that the output is a poor indicator of how many bits actually match the true vector. This true vector has 1s at positions $1, \ldots, 50$ and 0s at $51, \ldots, 100$.

Snoisy.py

```
import numpy as np

def Snoisy(X):   #takes a matrix
    n = X.shape[1]
    N = X.shape[0]
    # true binary vector
    xorg = np.hstack((np.ones((1,n//2)), np.zeros((1,n//2))))
    theta = 0.4 # probability to flip the input
    # storing the number of bits unequal to the true vector
    s = np.zeros(N)
    for i in range(0,N):
       # determine which bits to flip
       flip = (np.random.uniform(size=(n)) < theta).astype(int)
       ind = flip>0
       X[i][ind] = 1-X[i][ind]
       s[i] = (X[i] != xorg).sum()
    return s
```

The CE code below to optimize $S(\boldsymbol{x})$ is quite similar to the continuous optimization code in Example 3.16. However, instead of sampling iid random variables $X_1, \ldots, X_N$ from a normal distribution, we now sample iid binary vectors $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N$ from a $\mathsf{Ber}(\boldsymbol{p})$ distribution. More precisely, given a row vector of probabilities $\boldsymbol{p} = [p_1, \ldots, p_n]$, we independently simulate the components $X_1, \ldots, X_n$ of each binary vector $\boldsymbol{X}$ according to $X_i \sim \mathsf{Ber}(p_i)$, $i = 1, \ldots, n$. After each iteration, the vector $\boldsymbol{p}$ is updated as the (vector) mean of the elite

☞ 101

samples. The sample size is $N = 1000$ and the number of elite samples is 100. The components of the initial sampling vector $\boldsymbol{p}$ are all equal to $1/2$; that is, the $\boldsymbol{X}$ are initially uniformly sampled from the set of all binary vectors of length $n = 100$. At each subsequent iteration the parameter vector is updated via the mean of the elite samples and evolves towards a degenerate vector $\boldsymbol{p}^*$ with only 1s and 0s. Sampling from such a $\mathsf{Ber}(\boldsymbol{p}^*)$ distribution gives an outcome $\boldsymbol{x}^* = \boldsymbol{p}^*$, which can be taken as an estimate for the minimizer of S; that is, the true binary vector hidden in the black box. The algorithm stops when $\boldsymbol{p}$ has degenerated sufficiently.

Figure 3.16 shows the evolution of the vector of probabilities $\boldsymbol{p}$. This figure may be seen as the discrete analogue of Figure 3.12. We see that, despite the high noise, the CE method is able to find the true state of the black box, and hence the minimum value of S.

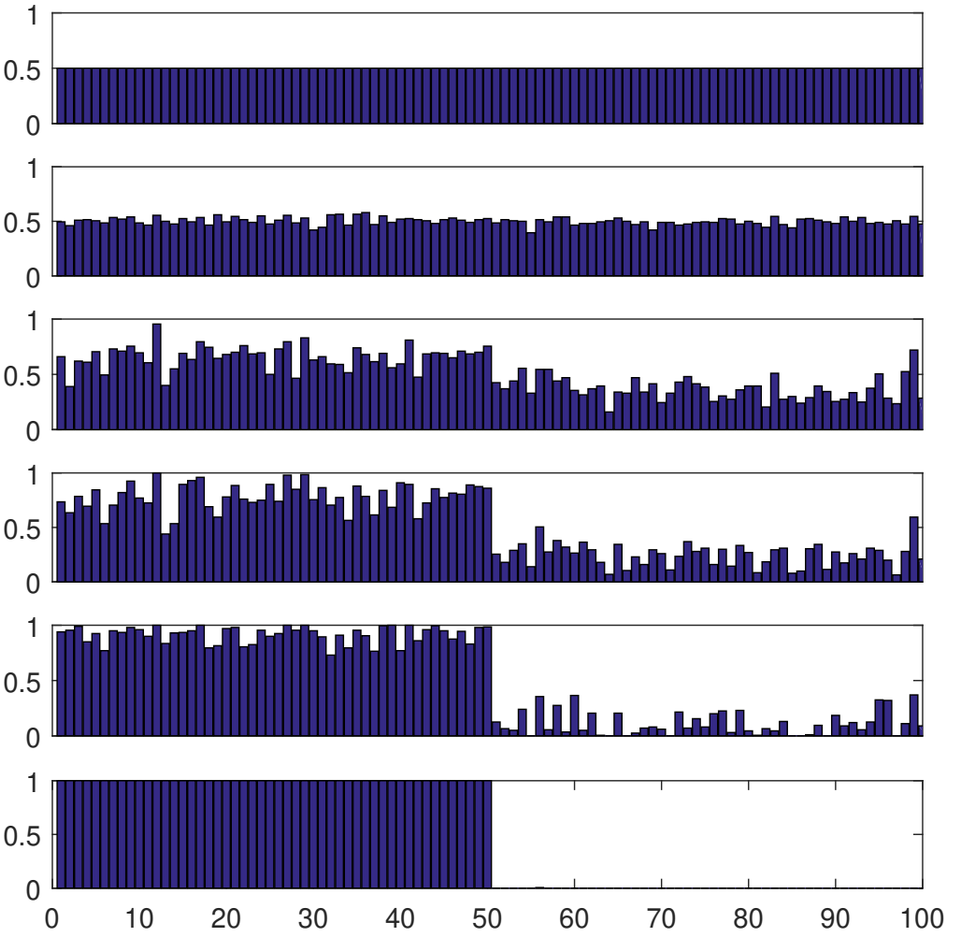


Figure 3.16: Evolution of the vector of probabilities $\boldsymbol{p} = [p_1, \ldots, p_n]$ towards the degenerate solution.

CEnoisy.py

```
from Snoisy import Snoisy
import numpy as np
n = 100
rho = 0.1
N = 1000; Nel = int(N*rho); eps = 0.01
p = 0.5*np.ones(n)
i = 0
pstart = p
ps = np.zeros((1000,n))
ps[0] = pstart
pdist = np.zeros((1,1000))
while np.max(np.minimum(p,1-p)) > eps:
    i += 1
    X = (np.random.uniform(size=(N,n)) < p).astype(int)
    X_tmp = np.array(X, copy=True)
    SX = Snoisy(X_tmp)
    ids = np.argsort(SX,axis=0)
    Elite = X[ids[0:Nel],:]
    p = np.mean(Elite,axis=0)
    ps[i] = p
print(p)
```

Further Reading

The article [68] explores why the Monte Carlo method is so important in today's quantitative investigations. The *Handbook of Monte Carlo Methods* [71] provides a comprehensive overview of Monte Carlo simulation that explores the latest topics, techniques, and real-world applications. Popular books on simulation and the Monte Carlo method include [42], [75], and [104]. A classic reference on random variable generation is [32]. Easy introductions to stochastic simulation are given in [49], [98], and [100]. More advanced theory can be found in [5]. Markov chain Monte Carlo is detailed in [50] and [99]. The research monograph on the cross-entropy method is [103] and a tutorial is provided in [30]. A range of optimization applications of the CE method is given in [16]. Theoretical results on adaptive tuning schemes for simulated annealing may be found, for example, in [111]. There are several established ways for gradient estimation. These include the finite difference method, infinitesimal perturbation analysis, the score function method, and the method of weak derivatives; see, for example, [51, Chapter 7].

Exercises

1. We can modify the Box–Muller method in Example 3.1 to draw X and Y uniformly on the unit disc, $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leqslant 1\}$, in the following way: Independently draw a radius R and an angle $\Theta \sim \mathcal{U}(0, 2\pi)$, and return $X = R\cos(\Theta)$, $Y = R\sin(\Theta)$. The question is how to draw R. ☞ 69

   (a) Show that the cdf of R is given by $F_R(r) = r^2$ for $0 \leqslant r \leqslant 1$ (with $F_R(r) = 0$ and

$F_R(r) = 1$ for $r < 0$ and $r > 1$, respectively).

(b) Explain how to simulate R using the inverse-transform method.

(c) Simulate 100 independent draws of $[X, Y]^\top$ according to the method described above.

2. A simple acceptance–rejection method to simulate a vector $\boldsymbol{X}$ in the unit d-ball $\{\boldsymbol{x} \in \mathbb{R}^d : \|\boldsymbol{x}\| \leqslant 1\}$ is to first generate $\boldsymbol{X}$ uniformly in the hyper cube $[-1, 1]^d$ and then to accept the point only if $\|\boldsymbol{X}\| \leqslant 1$. Determine an analytic expression for the probability of acceptance as a function of d and plot this for $d = 1, \ldots, 50$.

3. Let the random variable X have pdf

$$f(x) = \begin{cases} \frac{1}{2}\, x\,, & 0 \leqslant x < 1, \\ \frac{1}{2}\,, & 1 \leqslant x \leqslant \frac{5}{2}\,. \end{cases}$$

Simulate a random variable from $f(x)$, using

(a) the inverse-transform method;

(b) the acceptance–rejection method, using the proposal density

$$g(x) = \frac{8}{25}\, x\,, \quad 0 \leqslant x \leqslant \frac{5}{2}\,.$$

4. Construct simulation algorithms for the following distributions:

(a) The $\mathsf{Weib}(\alpha, \lambda)$ distribution, with cdf $F(x) = 1 - \mathrm{e}^{-(\lambda x)^\alpha}$, $x \geqslant 0$, where $\lambda > 0$ and $\alpha > 0$.

(b) The $\mathsf{Pareto}(\alpha, \lambda)$ distribution, with pdf $f(x) = \alpha\lambda(1 + \lambda x)^{-(\alpha+1)}$, $x \geqslant 0$, where $\lambda > 0$ and $\alpha > 0$.

5. We wish to sample from the pdf

$$f(x) = x\,\mathrm{e}^{-x}, \quad x \geqslant 0,$$

using acceptance–rejection with the proposal pdf $g(x) = \mathrm{e}^{-x/2}/2$, $x \geqslant 0$.

(a) Find the smallest C for which $Cg(x) \geqslant f(x)$ for all x.

(b) What is the efficiency of this acceptance–rejection method?

6. Let $[X, Y]^\top$ be uniformly distributed on the triangle with corners $(0, 0), (1, 2)$, and $(-1, 1)$. Give the distribution of $[U, V]^\top$ defined by the linear transformation

$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix}.$$

7. Explain how to generate a random variable from the *extreme value distribution*, which has cdf

$$F(x) = 1 - \mathrm{e}^{-\exp\left(\frac{x-\mu}{\sigma}\right)}\,, \quad -\infty < x < \infty, \quad (\sigma > 0),$$

via the inverse-transform method.

8. Write a program that generates and displays 100 random vectors that are uniformly distributed within the ellipse

$$5\,x^2 + 21\,x\,y + 25\,y^2 = 9.$$

[Hint: Consider generating uniformly distributed samples within the circle of radius 3 and use the fact that linear transformations preserve uniformity to transform the circle to the given ellipse.]

9. Suppose that $X_i \sim \mathsf{Exp}(\lambda_i)$, independently, for all $i = 1, \ldots, n$. Let $\mathbf{\Pi} = [\Pi_1, \ldots, \Pi_n]^\top$ be the random permutation induced by the ordering $X_{\Pi_1} < X_{\Pi_2} < \cdots < X_{\Pi_n}$, and define $Z_1 := X_{\Pi_1}$ and $Z_j := X_{\Pi_j} - X_{\Pi_{j-1}}$ for $j = 2, \ldots, n$.

   (a) Determine an $n \times n$ matrix $\mathbf{A}$ such that $\boldsymbol{Z} = \mathbf{A}\boldsymbol{X}$ and show that $\det(\mathbf{A}) = 1$.

   (b) Denote the joint pdf of $\boldsymbol{X}$ and $\mathbf{\Pi}$ as

$$f_{\boldsymbol{X},\mathbf{\Pi}}(\boldsymbol{x}, \boldsymbol{\pi}) = \prod_{i=1}^{n} \lambda_{\pi_i} \exp\left(-\lambda_{\pi_i} x_{\pi_i}\right) \times \mathbb{1}\{x_{\pi_1} < \cdots < x_{\pi_n}\}, \quad \boldsymbol{x} \geqslant \mathbf{0},\ \boldsymbol{\pi} \in \mathcal{P}_n,$$

   where $\mathcal{P}_n$ is the set of all $n!$ permutations of $\{1, \ldots, n\}$. Use the multivariate transformation formula (C.22) to show that ☞ 434

$$f_{\boldsymbol{Z},\mathbf{\Pi}}(\boldsymbol{z}, \boldsymbol{\pi}) = \exp\left(-\sum_{i=1}^{n} z_i \sum_{k \geqslant i} \lambda_{\pi_k}\right) \prod_{i=1}^{n} \lambda_i, \qquad \boldsymbol{z} \geqslant \mathbf{0},\ \boldsymbol{\pi} \in \mathcal{P}_n.$$

   Hence, conclude that the probability mass function of the random permutation $\mathbf{\Pi}$ is:

$$\mathbb{P}[\mathbf{\Pi} = \boldsymbol{\pi}] = \prod_{i=1}^{n} \frac{\lambda_{\pi_i}}{\sum_{k \geqslant i} \lambda_{\pi_k}}, \quad \boldsymbol{\pi} \in \mathcal{P}_n.$$

   (c) Write pseudo-code to simulate a *uniform* random permutation $\mathbf{\Pi} \in \mathcal{P}_n$; that is, such that $\mathbb{P}[\mathbf{\Pi} = \boldsymbol{\pi}] = \frac{1}{n!}$, and explain how this uniform random permutation can be used to reshuffle a training set τ_n.

10. Consider the Markov chain with transition graph given in Figure 3.17, starting in state 1.

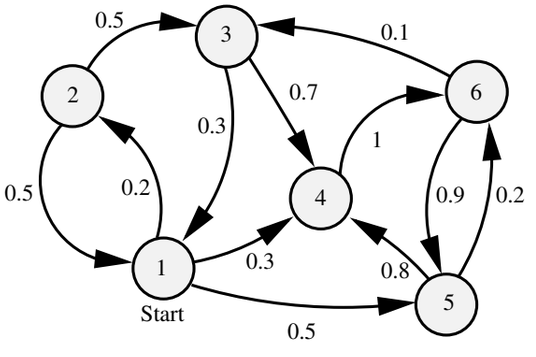


Figure 3.17: The transition graph for the Markov chain $\{X_t, t = 0, 1, 2, \ldots\}$.

(a) Construct a computer program to simulate the Markov chain, and show a realization for $N = 100$ steps.

(b) Compute the limiting probabilities that the Markov chain is in state 1,2,...,6, by solving the global balance equations (C.42).

☞ 454

(c) Verify that the exact limiting probabilities correspond to the average fraction of times that the Markov process visits states 1,2,...,6, for a large number of steps N.

11. As a generalization of Example C.9, consider a random walk on an arbitrary undirected connected graph with a finite vertex set $\mathcal{V}$. For any vertex $v \in \mathcal{V}$, let $d(v)$ be the number of neighbors of v — called the *degree* of v. The random walk can jump to each one of the neighbors with probability $1/d(v)$ and can be described by a Markov chain. Show that, if the chain is *aperiodic*, the limiting probability that the chain is in state v is equal to $d(v)/\sum_{v' \in \mathcal{V}} d(v')$.

☞ 455

12. Let $U, V \sim_{\text{iid}} \mathcal{U}(0,1)$. The reason why in Example 3.7 the sample mean and sample median behave very differently is that $\mathbb{E}[U/V] = \infty$, while the median of U/V is finite. Show this, and compute the median. [Hint: start by determining the cdf of $Z = U/V$ by writing it as an expectation of an indicator function.]

☞ 76

13. Consider the problem of generating samples from $Y \sim \mathsf{Gamma}(2, 10)$.

(a) Direct simulation: Let $U_1, U_2 \sim_{\text{iid}} \mathcal{U}(0,1)$. Show that $-\ln(U_1)/10 - \ln(U_2)/10 \sim \mathsf{Gamma}(2, 10)$. [Hint: derive the distribution of $-\ln(U_1)/10$ and use Example C.1.]

☞ 429

(b) Simulation via MCMC: Implement an independence sampler to simulate from the $\mathsf{Gamma}(2, 10)$ target pdf

$$f(x) = 100\, x\, \mathrm{e}^{-10x}, \quad x \geqslant 0,$$

using proposal transition density $q(y \,|\, x) = g(y)$, where $g(y)$ is the pdf of an $\mathsf{Exp}(5)$ random variable. Generate $N = 500$ samples, and compare the true cdf with the empirical cdf of the data.

14. Let $\boldsymbol{X} = [X, Y]^\top$ be a random column vector with a bivariate normal distribution with expectation vector $\boldsymbol{\mu} = [1, 2]^\top$ and covariance matrix

$$\boldsymbol{\Sigma} = \begin{bmatrix} 1 & a \\ a & 4 \end{bmatrix}.$$

(a) What are the conditional distributions of $(Y \,|\, X = x)$ and $(X \,|\, Y = y)$? [Hint: use Theorem C.8.]

☞ 438

(b) Implement a Gibbs sampler to draw 10^3 samples from the bivariate distribution $\mathcal{N}(\boldsymbol{\mu}, \Sigma)$ for $a = 0$, 1, and 1.75, and plot the resulting samples.

15. Here the objective is to sample from the 2-dimensional pdf

$$f(x, y) = c\, \mathrm{e}^{-(xy+x+y)}, \quad x \geqslant 0, \quad y \geqslant 0,$$

for some normalization constant c, using a Gibbs sampler. Let $(X, Y) \sim f$.

(a) Find the conditional pdf of X given $Y = y$, and the conditional pdf of Y given $X = x$.

(b) Write working Python code that implements the Gibbs sampler and outputs 1000 points that are approximately distributed according to f.

(c) Describe how the normalization constant c could be estimated via Monte Carlo simulation, using random variables $X_1, \ldots, X_N, Y_1, \ldots, Y_N \overset{\text{iid}}{\sim} \mathsf{Exp}(1)$.

16. We wish to estimate $\mu = \int_{-2}^{2} \mathrm{e}^{-x^2/2}\,\mathrm{d}x = \int H(x) f(x)\,\mathrm{d}x$ via Monte Carlo simulation using two different approaches: (1) defining $H(x) = 4\,\mathrm{e}^{-x^2/2}$ and f the pdf of the $\mathcal{U}[-2, 2]$ distribution and (2) defining $H(x) = \sqrt{2\pi}\,\mathbb{1}\{-2 \leqslant x \leqslant 2\}$ and f the pdf of the $\mathcal{N}(0, 1)$ distribution.

(a) For both cases estimate μ via the estimator $\widehat{\mu}$

$$\widehat{\mu} = N^{-1} \sum_{i=1}^{N} H(\boldsymbol{X}_i). \tag{3.34}$$

Use a sample size of $N = 1000$.

(b) For both cases estimate the relative error κ of $\widehat{\mu}$ using $N = 100$.

(c) Give a 95% confidence interval for μ for both cases using $N = 100$.

(d) From part (b), assess how large N should be such that the relative width of the confidence interval is less than 0.01, and carry out the simulation with this N. Compare the result with the true value of μ.

17. Consider estimation of the tail probability $\mu = \mathbb{P}[X \geqslant \gamma]$ of some random variable X, where γ is large. The crude Monte Carlo estimator of μ is

$$\widehat{\mu} = \frac{1}{N} \sum_{i=1}^{N} Z_i, \tag{3.35}$$

where $X_1, \ldots, X_N$ are iid copies of X and $Z_i = \mathbb{1}\{X_i \geqslant \gamma\}$, $i = 1, \ldots, N$.

(a) Show that $\widehat{\mu}$ is unbiased; that is, $\mathbb{E}\,\widehat{\mu} = \mu$.

(b) Express the relative error of $\widehat{\mu}$, i.e.,

$$\mathrm{RE} = \frac{\sqrt{\mathbb{V}\mathrm{ar}\,\widehat{\mu}}}{\mathbb{E}\,\widehat{\mu}},$$

in terms of N and μ.

(c) Explain how to estimate the relative error of $\widehat{\mu}$ from outcomes $x_1, \ldots, x_N$ of $X_1, \ldots, X_N$, and how to construct a 95% confidence interval for μ.

(d) An unbiased estimator Z of μ is said to be *logarithmically efficient* if

$$\lim_{\gamma \to \infty} \frac{\ln \mathbb{E} Z^2}{\ln \mu^2} = 1. \tag{3.36}$$

Show that the CMC estimator (3.35) with $N = 1$ is not logarithmically efficient.

18. One of the test cases in [70] involves the minimization of the *Hougen* function. Implement a cross-entropy and a simulated annealing algorithm to carry out this optimization task.

19. In the *binary knapsack problem*, the goal is to solve the optimization problem:

$$\max_{\boldsymbol{x}\in\{0,1\}^n} \boldsymbol{p}^\top \boldsymbol{x},$$

subject to the constraints

$$\mathbf{A}\boldsymbol{x} \leqslant \boldsymbol{c},$$

where $\boldsymbol{p}$ and $\boldsymbol{w}$ are $n \times 1$ vectors of non-negative numbers, $\mathbf{A} = (a_{ij})$ is an $m \times n$ matrix, and $\boldsymbol{c}$ is an $m \times 1$ vector. The interpretation is that $x_j = 1$ or 0 depending on whether item j with value p_j is packed into the knapsack or not , $j = 1, \ldots, n$; The variable a_{ij} represents the i-th attribute (e.g., volume, weight) of the j-th item. Associated with each attribute is a maximal capacity, e.g., c_1 could be the maximum volume of the knapsack, c_2 the maximum weight, etc.

Write a CE program to solve the `Sento1.dat` knapsack problem at http://people.brunel.ac.uk/~mastjjb/jeb/orlib/files/mknap2.txt, as described in [16].

20. Let $(C_1, R_1), (C_2, R_2), \ldots$ be a renewal reward process, with $\mathbb{E}R_1 < \infty$ and $\mathbb{E}C_1 < \infty$. Let $A_t = \sum_{i=1}^{N_t} R_i/t$ be the average reward at time $t = 1, 2, \ldots$, where $N_t = \max\{n : T_n \leqslant t\}$ and we have defined $T_n = \sum_{i=1}^{n} C_i$ as the time of the n-th renewal.

    (a) Show that $T_n/n \xrightarrow{\text{a.s.}} \mathbb{E}C_1$ as $n \to \infty$.

    (b) Show that $N_t \xrightarrow{\text{a.s.}} \infty$ as $t \to \infty$.

    (c) Show that $N_t/t \xrightarrow{\text{a.s.}} 1/\mathbb{E}C_1$ as $t \to \infty$. [Hint: Use the fact that $T_{N_t} \leqslant t \leqslant T_{N_t+1}$ for all $t = 1, 2, \ldots.$]

    (d) Show that

$$A_t \xrightarrow{\text{a.s.}} \frac{\mathbb{E}R_1}{\mathbb{E}C_1} \quad \text{as} \quad t \to \infty.$$

☞ 92

21. Prove Theorem 3.3.

☞ 96

22. Prove that if $H(\boldsymbol{x}) \geqslant 0$ the importance sampling pdf g^* in (3.22) gives the zero-variance importance sampling estimator $\widehat{\mu} = \mu$.

23. Let X and Y be random variables (not necessarily independent) and suppose we wish to estimate the expected difference $\mu = \mathbb{E}[X - Y] = \mathbb{E}X - \mathbb{E}Y$.

    (a) Show that if X and Y are *positively correlated*, the variance of $X - Y$ is smaller than if X and Y are *independent*.

    (b) Suppose now that X and Y have cdfs F and G, respectively, and are simulated via the inverse-transform method: $X = F^{-1}(U)$, $Y = G^{-1}(V)$, with $U, V \sim \mathcal{U}(0, 1)$, not necessarily independent. Intuitively, one might expect that

if U and V are positively correlated, the variance of $X-Y$ would be smaller than if U and V are independent. Show that this is not always the case by providing a counter-example.

(c) Continuing (b), assume now that F and G are continuous. Show that the variance of $X - Y$ by taking *common random numbers* $U = V$ is no larger than when U and V are independent. [Hint: Use the following lemma of Hoeffding [41]: If (X, Y) have joint cdf H with marginal cdfs of X and Y being F and G, respectively, then

$$\mathbb{C}\mathrm{ov}(X, Y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} (H(x, y) - F(x)\, G(y))\, \mathrm{d}x\, \mathrm{d}y,$$

provided $\mathbb{C}\mathrm{ov}(X, Y)$ exists.]

CHAPTER 4

UNSUPERVISED LEARNING

When there is no distinction between response and explanatory variables, unsupervised methods are required to learn the structure of the data. In this chapter we look at various unsupervised learning techniques, such as density estimation, clustering, and principal component analysis. Important tools in unsupervised learning include the cross-entropy training loss, mixture models, the Expectation–Maximization algorithm, and the Singular Value Decomposition.

4.1 Introduction

In contrast to supervised learning, where an "output" (response) variable y is explained by an "input" (explanatory) vector $\boldsymbol{x}$, in unsupervised learning there is no response variable and the overall goal is to extract useful information and patterns from the data, e.g., in the form $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ or as a matrix $\mathbf{X}^\top = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$. In essence, the objective of unsupervised learning is to learn about the underlying probability distribution of the data.

We start in Section 4.2 by setting up a framework for unsupervised learning that is similar to the framework used for supervised learning in Section 2.3. That is, we formulate unsupervised learning in terms of risk and loss minimization; but now involving the cross-entropy risk, rather than the squared-error risk. In a natural way this leads to fundamental learning concepts such as likelihood, Fisher information, and the Akaike information criterion. Section 4.3 introduces the Expectation–Maximization (EM) algorithm as a useful method for maximizing likelihood functions when their solution cannot be found easily in closed form.

☞ 23

If the data forms an iid sample from some unknown distribution, the "empirical distribution" of the data provides valuable information about the unknown distribution. In Section 4.4 we formalize the concept of the empirical distribution (a generalization of the empirical cdf) and explain how we can produce an estimate of the underlying probability density function of the data using kernel density estimators.

☞ 11

Most unsupervised learning techniques focus on identifying certain traits of the underlying distribution, such as its local maximizers. A related idea is to partition the data into clusters of points that are in some sense "similar" to each other. In Section 4.5 we formulate the clustering problem in terms of a mixture model. In particular, the data are assumed

☞ 135

to come from a mixture of (usually Gaussian) distributions, and the objective is to recover the parameters of the mixture distributions from the data. The principal tool for parameter estimation in mixture models is the EM algorithm.

Section 4.6 discusses a more heuristic approach to clustering, where the data are grouped according to certain "cluster centers", whose positions are found by solving an optimization problem. Section 4.7 describes how clusters can be constructed in a hierarchical manner.

Finally, in Section 4.8 we discuss the unsupervised learning technique called Principal Component Analysis (PCA), which is an important tool for reducing the dimensionality of the data.

We will revisit various unsupervised learning techniques in subsequent chapters on *supervised* learning. For example, cross-entropy training loss minimization will be important in logistic regression (Section 5.7) and classification (Chapter 7), and PCA can be used for variable selection and dimensionality reduction, to make models easier to train and increase their predictive power; see e.g., Sections 6.8 and 7.4.

☞ 204
☞ 253

4.2 Risk and Loss in Unsupervised Learning

In unsupervised learning, the training data $\mathcal{T} := \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n\}$ only consists of (what are usually assumed to be) independent copies of a feature vector $\boldsymbol{X}$; there is no response data. Suppose our objective is to learn the unknown pdf f of $\boldsymbol{X}$ based on an outcome $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ of the training data $\mathcal{T}$. Conveniently, we can follow the same line of reasoning as for *supervised* learning, discussed in Sections 2.3–2.5. Table 4.1 gives a summary of definitions for the case of unsupervised learning. Compare this with Table 2.1 for the supervised case.

☞ 23
☞ 25

Similar to supervised learning, we wish to find a function g, which is now a probability density (continuous or discrete), that best approximates the pdf f in terms of minimizing a risk

$$\ell(g) := \mathbb{E}\,\mathrm{Loss}(f(\boldsymbol{X}), g(\boldsymbol{X})), \tag{4.1}$$

where Loss is a loss function. In (2.27), we already encountered the Kullback–Leibler risk

$$\ell(g) := \mathbb{E} \ln \frac{f(\boldsymbol{X})}{g(\boldsymbol{X})} = \mathbb{E} \ln f(\boldsymbol{X}) - \mathbb{E} \ln g(\boldsymbol{X}). \tag{4.2}$$

If $\mathcal{G}$ is a class of functions that contains f, then minimizing the Kullback–Leibler risk over $\mathcal{G}$ will yield the (correct) minimizer f. Of course, the problem is that minimization of (4.2) depends on f, which is generally not known. However, since the term $\mathbb{E} \ln f(\boldsymbol{X})$ does not depend on g, it plays no role in the minimization of the Kullback–Leibler risk. By removing this term, we obtain the *cross-entropy risk* (for discrete $\boldsymbol{X}$ replace the integral with a sum):

CROSS-ENTROPY RISK

$$\ell(g) := -\mathbb{E} \ln g(\boldsymbol{X}) = -\int f(\boldsymbol{x}) \ln g(\boldsymbol{x})\, \mathrm{d}\boldsymbol{x}. \tag{4.3}$$

Thus, minimizing the cross-entropy risk (4.3) over all $g \in \mathcal{G}$, again gives the minimizer f, provided that $f \in \mathcal{G}$. Unfortunately, solving (4.3) is also infeasible in general, as it still

Table 4.1: Summary of definitions for unsupervised learning.

$\boldsymbol{x}$	Fixed feature vector.
$\boldsymbol{X}$	Random feature vector.
$f(\boldsymbol{x})$	Pdf of $\boldsymbol{X}$ evaluated at the point $\boldsymbol{x}$.
τ or τ_n	Fixed training data $\{\boldsymbol{x}_i, i = 1, \ldots, n\}$.
$\mathcal{T}$ or $\mathcal{T}_n$	Random training data $\{\boldsymbol{X}_i, i = 1, \ldots, n\}$.
g	Approximation of the pdf f.
$\text{Loss}(f(\boldsymbol{x}), g(\boldsymbol{x}))$	Loss incurred when approximating $f(\boldsymbol{x})$ with $g(\boldsymbol{x})$.
$\ell(g)$	Risk for approximation function g; that is, $\mathbb{E}\,\text{Loss}(f(\boldsymbol{X}), g(\boldsymbol{X}))$.
$g^{\mathcal{G}}$	Optimal approximation function in function class $\mathcal{G}$; that is, $\text{argmin}_{g\in\mathcal{G}}\, \ell(g)$.
$\ell_\tau(g)$	Training loss for approximation function (guess) g; that is, the sample average estimate of $\ell(g)$ based on a fixed training sample τ.
$\ell_{\mathcal{T}}(g)$	The same as $\ell_\tau(g)$, but now for a random training sample $\mathcal{T}$.
$g_\tau^{\mathcal{G}}$ or g_τ	The *learner*: $\text{argmin}_{g\in\mathcal{G}}\, \ell_\tau(g)$. That is, the optimal approximation function based on a fixed training set τ and function class $\mathcal{G}$. We suppress the superscript $\mathcal{G}$ if the function class is implicit.
$g_{\mathcal{T}}^{\mathcal{G}}$ or $g_{\mathcal{T}}$	The learner for a random training set $\mathcal{T}$.

depends on f. Instead, we seek to minimize the *cross-entropy training loss*:

CROSS-ENTROPY TRAINING LOSS

$$\ell_\tau(g) := \frac{1}{n}\sum_{i=1}^{n} \text{Loss}(f(\boldsymbol{x}_i), g(\boldsymbol{x}_i)) = -\frac{1}{n}\sum_{i=1}^{n} \ln g(\boldsymbol{x}_i) \tag{4.4}$$

over the class of functions $\mathcal{G}$, where $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ is an iid sample from f. This optimization is doable without knowing f and is equivalent to solving the maximization problem

$$\max_{g\in\mathcal{G}} \sum_{i=1}^{n} \ln g(\boldsymbol{x}_i). \tag{4.5}$$

A key step in setting up the learning procedure is to select a suitable function class $\mathcal{G}$ over which to optimize. The standard approach is to parameterize g with a parameter $\boldsymbol{\theta}$ and let $\mathcal{G}$ be the class of functions $\{g(\cdot\,|\,\boldsymbol{\theta}), \boldsymbol{\theta} \in \Theta\}$ for some p-dimensional parameter set Θ. For the remainder of Section 4.2, we will be using this function class, as well as the cross-entropy risk.

The function $\boldsymbol{\theta} \mapsto g(\boldsymbol{x}\,|\,\boldsymbol{\theta})$ is called the *likelihood function*. It gives the likelihood of the observed feature vector $\boldsymbol{x}$ under $g(\cdot\,|\,\boldsymbol{\theta})$, as a function of the parameter $\boldsymbol{\theta}$. The natural logarithm of the likelihood function is called the *log-likelihood* function and its gradient with respect to $\boldsymbol{\theta}$ is called the *score function*, denoted $\boldsymbol{S}(\boldsymbol{x}\,|\,\boldsymbol{\theta})$; that is,

LIKELIHOOD FUNCTION

SCORE FUNCTION

$$\boldsymbol{S}(\boldsymbol{x}\,|\,\boldsymbol{\theta}) := \frac{\partial \ln g(\boldsymbol{x}\,|\,\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} = \frac{\frac{\partial g(\boldsymbol{x}\,|\,\boldsymbol{\theta})}{\partial \boldsymbol{\theta}}}{g(\boldsymbol{x}\,|\,\boldsymbol{\theta})}. \tag{4.6}$$

The random score $\boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta})$, with $\boldsymbol{X} \sim g(\cdot \,|\, \boldsymbol{\theta})$, is of particular interest. In many cases, its expectation is *equal to the zero vector*; namely,

$$\begin{aligned} \mathbb{E}_{\boldsymbol{\theta}} \boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta}) &= \int \frac{\frac{\partial g(\boldsymbol{x} \,|\, \boldsymbol{\theta})}{\partial \boldsymbol{\theta}}}{g(\boldsymbol{x} \,|\, \boldsymbol{\theta})} \, g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{x} \\ &= \int \frac{\partial g(\boldsymbol{x} \,|\, \boldsymbol{\theta})}{\partial \boldsymbol{\theta}} \, \mathrm{d}\boldsymbol{x} = \frac{\partial \int g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{x}}{\partial \boldsymbol{\theta}} = \frac{\partial 1}{\partial \boldsymbol{\theta}} = \mathbf{0}, \end{aligned} \tag{4.7}$$

provided that the interchange of differentiation and integration is justified. This is true for a large number of distributions, including the normal, exponential, and binomial distributions. Notable exceptions are distributions whose support depends on the distributional parameter; for example the $\mathcal{U}(0, \theta)$ distribution.

It is important to see whether expectations are taken with respect to $\boldsymbol{X} \sim g(\cdot \,|\, \boldsymbol{\theta})$ or $\boldsymbol{X} \sim f$. We use the expectation symbols $\mathbb{E}_{\boldsymbol{\theta}}$ and $\mathbb{E}$ to distinguish the two cases.

From now on we simply assume that the interchange of differentiation and integration is permitted; see, e.g., [76] for sufficient conditions. The covariance matrix of the random score $\boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta})$ is called the *Fisher information matrix*, which we denote by $\mathbf{F}$ or $\mathbf{F}(\boldsymbol{\theta})$ to show its dependence on $\boldsymbol{\theta}$. Since the expected score is $\mathbf{0}$, we have

FISHER INFORMATION MATRIX

$$\mathbf{F}(\boldsymbol{\theta}) = \mathbb{E}_{\boldsymbol{\theta}}[\boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta}) \, \boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta})^{\top}]. \tag{4.8}$$

☞ 400

A related matrix is the expected Hessian matrix of $-\ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})$:

$$\mathbf{H}(\boldsymbol{\theta}) := \mathbb{E}\left[-\frac{\partial \boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \boldsymbol{\theta}}\right] = -\mathbb{E}\begin{bmatrix} \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial^2 \theta_1} & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_1 \partial \theta_2} & \cdots & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_1 \partial \theta_p} \\ \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_2 \partial \theta_1} & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial^2 \theta_2} & \cdots & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_2 \partial \theta_p} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_p \partial \theta_1} & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial \theta_p \partial \theta_2} & \cdots & \frac{\partial^2 \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta})}{\partial^2 \theta_p} \end{bmatrix}. \tag{4.9}$$

Note that the expectation here is with respect to $\boldsymbol{X} \sim f$. It turns out that if $f = g(\cdot \,|\, \boldsymbol{\theta})$, the two matrices are the *same*; that is,

$$\mathbf{F}(\boldsymbol{\theta}) = \mathbf{H}(\boldsymbol{\theta}), \tag{4.10}$$

provided that we may swap the order of differentiation and integration (expectation). This result is called the *information matrix equality*. We leave the proof as Exercise 1.

INFORMATION MATRIX EQUALITY

The matrices $\mathbf{F}(\boldsymbol{\theta})$ and $\mathbf{H}(\boldsymbol{\theta})$ play important roles in approximating the cross-entropy risk for large n. To set the scene, let $g^{\mathcal{G}} = g(\cdot \,|\, \boldsymbol{\theta}^*)$ be the minimizer of the cross-entropy risk

$$r(\boldsymbol{\theta}) := -\mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}).$$

We assume that r, as a function of $\boldsymbol{\theta}$, is well-behaved; in particular, that in the neighborhood of $\boldsymbol{\theta}^*$ it is strictly convex and twice continuously differentiable (this holds true, for example, if g is a Gaussian density). It follows that $\boldsymbol{\theta}^*$ is a root of $\mathbb{E}\, \boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta})$, because

$$\mathbf{0} = \frac{\partial r(\boldsymbol{\theta}^*)}{\partial \boldsymbol{\theta}} = -\frac{\partial \, \mathbb{E} \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}^*)}{\partial \boldsymbol{\theta}} = -\mathbb{E} \frac{\partial \ln g(\boldsymbol{X} \,|\, \boldsymbol{\theta}^*)}{\partial \boldsymbol{\theta}} = -\mathbb{E}\, \boldsymbol{S}(\boldsymbol{X} \,|\, \boldsymbol{\theta}^*),$$

again provided that the order of differentiation and integration (expectation) can be swapped. In the same way, $\mathbf{H}(\boldsymbol{\theta})$ is then the Hessian matrix of r. Let $g(\cdot \,|\, \widehat{\boldsymbol{\theta}}_n)$ be the minimizer of the training loss

$$r_{\mathcal{T}_n}(\boldsymbol{\theta}) := -\frac{1}{n}\sum_{i=1}^{n} \ln g(\boldsymbol{X}_i \,|\, \boldsymbol{\theta}),$$

where $\mathcal{T}_n = \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n\}$ is a random training set. Let r^* be the smallest possible cross-entropy risk, taken over all functions; clearly, $r^* = -\mathbb{E} \ln f(\boldsymbol{X})$, where $\boldsymbol{X} \sim f$. Similar to the supervised learning case, we can decompose the generalization risk, $\ell(g(\cdot \,|\, \widehat{\boldsymbol{\theta}}_n)) = r(\widehat{\boldsymbol{\theta}}_n)$, into

$$r(\widehat{\boldsymbol{\theta}}_n) = r^* + \underbrace{r(\boldsymbol{\theta}^*) - r^*}_{\text{approx. error}} + \underbrace{r(\widehat{\boldsymbol{\theta}}_n) - r(\boldsymbol{\theta}^*)}_{\text{statistical error}} = r(\boldsymbol{\theta}^*) - \mathbb{E} \ln \frac{g(\boldsymbol{X} \,|\, \boldsymbol{\theta}^*)}{g(\boldsymbol{X} \,|\, \widehat{\boldsymbol{\theta}}_n)}.$$

The following theorem specifies the asymptotic behavior of the components of the generalization risk. In the proof we assume that $\widehat{\boldsymbol{\theta}}_n \xrightarrow{\mathbb{P}} \boldsymbol{\theta}^*$ as $n \to \infty$. ☞ 441

Theorem 4.1: Approximating the Cross-Entropy Risk

It holds asymptotically ($n \to \infty$) that

$$\mathbb{E} r(\widehat{\boldsymbol{\theta}}_n) - r(\boldsymbol{\theta}^*) \simeq \operatorname{tr}\left(\mathbf{F}(\boldsymbol{\theta}^*)\, \mathbf{H}^{-1}(\boldsymbol{\theta}^*)\right)/(2n), \tag{4.11}$$

where

$$r(\boldsymbol{\theta}^*) \simeq \mathbb{E} r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + \operatorname{tr}\left(\mathbf{F}(\boldsymbol{\theta}^*)\, \mathbf{H}^{-1}(\boldsymbol{\theta}^*)\right)/(2n). \tag{4.12}$$

Proof: A Taylor expansion of $r(\widehat{\boldsymbol{\theta}}_n)$ around $\boldsymbol{\theta}^*$ gives the statistical error ☞ 402

$$r(\widehat{\boldsymbol{\theta}}_n) - r(\boldsymbol{\theta}^*) = (\widehat{\boldsymbol{\theta}}_n - \boldsymbol{\theta}^*)^\top \underbrace{\frac{\partial r(\boldsymbol{\theta}^*)}{\partial \boldsymbol{\theta}}}_{=\mathbf{0}} + \frac{1}{2}(\widehat{\boldsymbol{\theta}}_n - \boldsymbol{\theta}^*)^\top \mathbf{H}(\bar{\boldsymbol{\theta}}_n)(\widehat{\boldsymbol{\theta}}_n - \boldsymbol{\theta}^*), \tag{4.13}$$

where $\bar{\boldsymbol{\theta}}_n$ lies on the line segment between $\boldsymbol{\theta}^*$ and $\widehat{\boldsymbol{\theta}}_n$. For large n we may replace $\mathbf{H}(\bar{\boldsymbol{\theta}}_n)$ with $\mathbf{H}(\boldsymbol{\theta}^*)$ as, by assumption, $\bar{\boldsymbol{\theta}}_n$ converges to $\boldsymbol{\theta}^*$. The matrix $\mathbf{H}(\boldsymbol{\theta}^*)$ is positive definite because $r(\boldsymbol{\theta})$ is strictly convex at $\boldsymbol{\theta}^*$ by assumption, and therefore invertible. It is important to realize that $\widehat{\boldsymbol{\theta}}_n$ is in fact an M-estimator of $\boldsymbol{\theta}^*$. In particular, in the notation of Theorem C.19, we have $\boldsymbol{\psi} = \boldsymbol{S}$, $\mathbf{A} = \mathbf{H}(\boldsymbol{\theta}^*)$, and $\mathbf{B} = \mathbf{F}(\boldsymbol{\theta}^*)$. Consequently, by that same theorem, ☞ 451

$$\sqrt{n}\,(\widehat{\boldsymbol{\theta}}_n - \boldsymbol{\theta}^*) \xrightarrow{\mathrm{d}} \mathcal{N}\left(\mathbf{0}, \mathbf{H}^{-1}(\boldsymbol{\theta}^*)\, \mathbf{F}(\boldsymbol{\theta}^*)\, \mathbf{H}^{-\top}(\boldsymbol{\theta}^*)\right). \tag{4.14}$$

Combining (4.13) with (4.14), it follows from Theorem C.2 that asymptotically the expected estimation error is given by (4.11). ☞ 432

Next, we consider a Taylor expansion of $r_{\mathcal{T}_n}(\boldsymbol{\theta}^*)$ around $\widehat{\boldsymbol{\theta}}_n$:

$$r_{\mathcal{T}_n}(\boldsymbol{\theta}^*) = r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + (\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n)^\top \underbrace{\frac{\partial r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n)}{\partial \boldsymbol{\theta}}}_{=\mathbf{0}} + \frac{1}{2}(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n)^\top \mathbf{H}_{\mathcal{T}_n}(\bar{\boldsymbol{\theta}}_n)(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n), \tag{4.15}$$

where $\mathbf{H}_{\mathcal{T}_n}(\overline{\boldsymbol{\theta}}_n) := -\frac{1}{n}\sum_{i=1}^n \frac{\partial S(\boldsymbol{X}_i \,|\, \overline{\boldsymbol{\theta}}_n)}{\partial \boldsymbol{\theta}}$ is the Hessian of $r_{\mathcal{T}_n}(\boldsymbol{\theta})$ at some $\overline{\boldsymbol{\theta}}_n$ between $\widehat{\boldsymbol{\theta}}_n$ and $\boldsymbol{\theta}^*$. Taking expectations on both sides of (4.15), we obtain

$$r(\boldsymbol{\theta}^*) = \mathbb{E} r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + \frac{1}{2}\mathbb{E}\,(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n)^\top \mathbf{H}_{\mathcal{T}_n}(\overline{\boldsymbol{\theta}}_n)(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n).$$

Replacing $\mathbf{H}_{\mathcal{T}_n}(\overline{\boldsymbol{\theta}}_n)$ with $\mathbf{H}(\boldsymbol{\theta}^*)$ for large n and using (4.14), we have

$$n\,\mathbb{E}\,(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n)^\top \mathbf{H}_{\mathcal{T}_n}(\overline{\boldsymbol{\theta}}_n)(\boldsymbol{\theta}^* - \widehat{\boldsymbol{\theta}}_n) \longrightarrow \operatorname{tr}\left(\mathbf{F}(\boldsymbol{\theta}^*)\,\mathbf{H}^{-1}(\boldsymbol{\theta}^*)\right), \quad n \to \infty.$$

Therefore, asymptotically as $n \to \infty$, we have (4.12). □

Theorem 4.1 has a number of interesting consequences:

☞ 35

1. Similar to Section 2.5.1, the training loss $\ell_{\mathcal{T}_n}(g_{\mathcal{T}_n}) = r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n)$ tends to underestimate the risk $\ell(g^{\mathcal{G}}) = r(\boldsymbol{\theta}^*)$, because the training set $\mathcal{T}_n$ is used to both train $g \in \mathcal{G}$ (that is, estimate $\boldsymbol{\theta}^*$) and to estimate the risk. The relation (4.12) tells us that on average the training loss underestimates the true risk by $\operatorname{tr}(\mathbf{F}(\boldsymbol{\theta}^*)\,\mathbf{H}^{-1}(\boldsymbol{\theta}^*))/(2n)$.

2. Adding equations (4.11) and (4.12), yields the following asymptotic approximation to the expected generalization risk:

$$\mathbb{E}\, r(\widehat{\boldsymbol{\theta}}_n) \simeq \mathbb{E}\, r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + \frac{1}{n}\operatorname{tr}\left(\mathbf{F}(\boldsymbol{\theta}^*)\,\mathbf{H}^{-1}(\boldsymbol{\theta}^*)\right) \tag{4.16}$$

The first term on the right-hand side of (4.16) can be estimated (without bias) via the training loss $r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n)$. As for the second term, we have already mentioned that when the true model $f \in \mathcal{G}$, then $\mathbf{F}(\boldsymbol{\theta}^*) = \mathbf{H}(\boldsymbol{\theta}^*)$. Therefore, when $\mathcal{G}$ is deemed to be a sufficiently rich class of models parameterized by a p-dimensional vector $\boldsymbol{\theta}$, we may approximate the second term as $\operatorname{tr}(\mathbf{F}(\boldsymbol{\theta}^*)\mathbf{H}^{-1}(\boldsymbol{\theta}^*))/n \approx \operatorname{tr}(\mathbf{I}_p)/n = p/n$. This suggests the following heuristic approximation to the (expected) generalization risk:

$$\mathbb{E}\, r(\widehat{\boldsymbol{\theta}}_n) \approx r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + \frac{p}{n}. \tag{4.17}$$

3. Multiplying both sides of (4.16) by $2n$ and substituting $\operatorname{tr}\left(\mathbf{F}(\boldsymbol{\theta}^*)\mathbf{H}^{-1}(\boldsymbol{\theta}^*)\right) \approx p$, we obtain the approximation:

$$2n\, r(\widehat{\boldsymbol{\theta}}_n) \approx -2\sum_{i=1}^n \ln g(\boldsymbol{X}_i \,|\, \widehat{\boldsymbol{\theta}}_n) + 2p. \tag{4.18}$$

AKAIKE INFORMATION CRITERION

The right-hand side of (4.18) is called the *Akaike information criterion* (AIC). Just like (4.17), the AIC approximation can be used to compare the difference in generalization risk of two or more learners. We prefer the learner with the smallest (estimated) generalization risk.

Suppose that, for a training set $\mathcal{T}$, the training loss $r_{\mathcal{T}}(\boldsymbol{\theta})$ has a unique minimum point $\widehat{\boldsymbol{\theta}}$ which lies in the interior of Θ. If $r_{\mathcal{T}}(\boldsymbol{\theta})$ is a differentiable function with respect to $\boldsymbol{\theta}$, then we can find the optimal parameter $\widehat{\boldsymbol{\theta}}$ by solving

$$\frac{\partial r_{\mathcal{T}}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} = \underbrace{\frac{1}{n}\sum_{i=1}^n \boldsymbol{S}(\boldsymbol{X}_i \,|\, \boldsymbol{\theta})}_{\boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta})} = \mathbf{0}.$$

In other words, the maximum likelihood estimate $\widehat{\boldsymbol{\theta}}$ for $\boldsymbol{\theta}$ is obtained by solving the root of the average score function, that is, by solving

$$\boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta}) = \mathbf{0}. \tag{4.19}$$

It is often not possible to find $\widehat{\boldsymbol{\theta}}$ in an explicit form. In that case one needs to solve the equation (4.19) numerically. There exist many standard techniques for root-finding, e.g., via *Newton's method* (see Section B.3.1), whereby, starting from an initial guess $\boldsymbol{\theta}_0$, subsequent iterates are obtained via the iterative scheme

NEWTON'S METHOD

☞ 411

$$\boldsymbol{\theta}_{t+1} = \boldsymbol{\theta}_t + \mathbf{H}_{\mathcal{T}}^{-1}(\boldsymbol{\theta}_t)\, \boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta}_t),$$

where

$$\mathbf{H}_{\mathcal{T}}(\boldsymbol{\theta}) := \frac{-\partial \boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} = \frac{1}{n}\sum_{i=1}^{n} -\frac{\partial \boldsymbol{S}(\boldsymbol{X}_i \,|\, \boldsymbol{\theta})}{\partial \boldsymbol{\theta}}$$

is the average Hessian matrix of $\{-\ln g(\boldsymbol{X}_i \,|\, \boldsymbol{\theta})\}_{i=1}^n$. Under $f = g(\cdot \,|\, \boldsymbol{\theta})$, the expectation of $\mathbf{H}_{\mathcal{T}}(\boldsymbol{\theta})$ is equal to the information matrix $\mathbf{F}(\boldsymbol{\theta})$, which does not depend on the data. This suggests an alternative iterative scheme, called *Fisher's scoring method*:

FISHER'S SCORING METHOD

$$\boldsymbol{\theta}_{t+1} = \boldsymbol{\theta}_t + \mathbf{F}^{-1}(\boldsymbol{\theta}_t)\, \boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta}_t), \tag{4.20}$$

which is not only easier to implement (if the information matrix can be readily evaluated), but also is more numerically stable.

■ **Example 4.1 (Maximum Likelihood for the Gamma Distribution)** We wish to approximate the density of the Gamma(α^*, λ^*) distribution for some true but unknown parameters α^* and λ^*, on the basis of a training set $\tau = \{x_1, \ldots, x_n\}$ of iid samples from this distribution. Choosing our approximating function $g(\cdot \,|\, \alpha, \lambda)$ in the same class of gamma densities,

$$g(x \,|\, \alpha, \lambda) = \frac{\lambda^\alpha x^{\alpha-1} \mathrm{e}^{-\lambda x}}{\Gamma(\alpha)}, \quad x \geqslant 0, \tag{4.21}$$

with $\alpha > 0$ and $\lambda > 0$, we seek to solve (4.19). Taking the logarithm in (4.21), the log-likelihood function is given by

$$l(x \,|\, \alpha, \lambda) := \alpha \ln \lambda - \ln \Gamma(\alpha) + (\alpha - 1) \ln x - \lambda x.$$

It follows that

$$\boldsymbol{S}(\alpha, \lambda) = \begin{bmatrix} \frac{\partial}{\partial \alpha} l(x \,|\, \alpha, \lambda) \\ \frac{\partial}{\partial \lambda} l(x \,|\, \alpha, \lambda) \end{bmatrix} = \begin{bmatrix} \ln \lambda - \psi(\alpha) + \ln x \\ \frac{\alpha}{\lambda} - x \end{bmatrix},$$

where ψ is the derivative of $\ln \Gamma$: the so-called *digamma function*. Hence,

DIGAMMA FUNCTION

$$\mathbf{H}(\alpha, \lambda) = -\mathbb{E}\begin{bmatrix} \frac{\partial^2}{\partial \alpha^2} l(X \,|\, \alpha, \lambda) & \frac{\partial^2}{\partial \alpha \partial \lambda} l(X \,|\, \alpha, \lambda) \\ \frac{\partial^2}{\partial \alpha \partial \lambda} l(X \,|\, \alpha, \lambda) & \frac{\partial^2}{\partial \lambda^2} l(X \,|\, \alpha, \lambda) \end{bmatrix} = -\mathbb{E}\begin{bmatrix} -\psi'(\alpha) & \frac{1}{\lambda} \\ \frac{1}{\lambda} & -\frac{\alpha}{\lambda^2} \end{bmatrix} = \begin{bmatrix} \psi'(\alpha) & -\frac{1}{\lambda} \\ -\frac{1}{\lambda} & \frac{\alpha}{\lambda^2} \end{bmatrix}.$$

Fisher's scoring method (4.20) can now be used to solve (4.19), with

$$\boldsymbol{S}_\tau(\alpha, \lambda) = \begin{bmatrix} \ln \lambda - \psi(\alpha) + n^{-1} \sum_{i=1}^n \ln x_i \\ \frac{\alpha}{\lambda} - n^{-1} \sum_{i=1}^n x_i \end{bmatrix}$$

and $\mathbf{F}(\alpha, \lambda) = \mathbf{H}(\alpha, \lambda)$. ■

4.3 Expectation–Maximization (EM) Algorithm

The *Expectation–Maximization* algorithm (EM) is a general algorithm for maximization of complicated (log-)likelihood functions, through the introduction of auxiliary variables.

To simplify the notation in this section, we use a Bayesian notation system, where the same symbol is used for different (conditional) probability densities.

As in the previous section, given independent observations $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ from some unknown pdf f, the objective is to find the best approximation to f in a function class $\mathcal{G} = \{g(\cdot \,|\, \boldsymbol{\theta}), \boldsymbol{\theta} \in \Theta\}$ by solving the maximum likelihood problem:

$$\boldsymbol{\theta}^* = \operatorname*{argmax}_{\boldsymbol{\theta} \in \Theta} g(\tau \,|\, \boldsymbol{\theta}), \tag{4.22}$$

where $g(\tau \,|\, \boldsymbol{\theta}) := g(\boldsymbol{x}_1 \,|\, \boldsymbol{\theta}) \cdots g(\boldsymbol{x}_n \,|\, \boldsymbol{\theta})$. The key element of the EM algorithm is the augmentation of the data τ with a suitable vector of *latent variables*, z, such that

LATENT VARIABLES

$$g(\tau \,|\, \boldsymbol{\theta}) = \int g(\tau, z \,|\, \boldsymbol{\theta}) \, \mathrm{d}z.$$

COMPLETE-DATA LIKELIHOOD

The function $\boldsymbol{\theta} \mapsto g(\tau, z \,|\, \boldsymbol{\theta})$ is usually referred to as the *complete-data likelihood* function. The choice of the latent variables is guided by the desire to make the maximization of $g(\tau, z \,|\, \boldsymbol{\theta})$ much easier than that of $g(\tau \,|\, \boldsymbol{\theta})$.

Suppose p denotes an arbitrary density of the latent variables z. Then, we can write:

$$\begin{aligned}
\ln g(\tau \,|\, \boldsymbol{\theta}) &= \int p(z) \ln g(\tau \,|\, \boldsymbol{\theta}) \, \mathrm{d}z \\
&= \int p(z) \ln \left(\frac{g(\tau, z \,|\, \boldsymbol{\theta}) / p(z)}{g(z \,|\, \tau, \boldsymbol{\theta}) / p(z)} \right) \mathrm{d}z \\
&= \int p(z) \ln \left(\frac{g(\tau, z \,|\, \boldsymbol{\theta})}{p(z)} \right) \mathrm{d}z - \int p(z) \ln \left(\frac{g(z \,|\, \tau, \boldsymbol{\theta})}{p(z)} \right) \mathrm{d}z \\
&= \int p(z) \ln \left(\frac{g(\tau, z \,|\, \boldsymbol{\theta})}{p(z)} \right) \mathrm{d}z + \mathcal{D}(p, g(\cdot \,|\, \tau, \boldsymbol{\theta})),
\end{aligned} \tag{4.23}$$

☞ 42

where $\mathcal{D}(p, g(\cdot \,|\, \tau, \boldsymbol{\theta}))$ is the Kullback–Leibler divergence from the density p to $g(\cdot \,|\, \tau, \boldsymbol{\theta})$. Since $\mathcal{D} \geqslant 0$, it follows that

$$\ln g(\tau \,|\, \boldsymbol{\theta}) \geqslant \int p(z) \ln \left(\frac{g(\tau, z \,|\, \boldsymbol{\theta})}{p(z)} \right) \mathrm{d}z =: \mathcal{L}(p, \boldsymbol{\theta})$$

for all $\boldsymbol{\theta}$ and any density p of the latent variables. In other words, $\mathcal{L}(p, \boldsymbol{\theta})$ is a lower bound on the log-likelihood that involves the complete-data likelihood. The EM algorithm then aims to increase this lower bound as much as possible by starting with an initial guess $\boldsymbol{\theta}^{(0)}$ and then, for $t = 1, 2, \ldots$, solving the following two steps:

1. $p^{(t)} = \operatorname{argmax}_p \mathcal{L}(p, \boldsymbol{\theta}^{(t-1)})$,
2. $\boldsymbol{\theta}^{(t)} = \operatorname{argmax}_{\boldsymbol{\theta} \in \Theta} \mathcal{L}(p^{(t)}, \boldsymbol{\theta})$.

The first optimization problem can be solved explicitly. Namely, by (4.23), we have that

$$p^{(t)} = \operatorname*{argmin}_{p} \mathcal{D}(p, g(\cdot \mid \tau, \boldsymbol{\theta}^{(t-1)})) = g(\cdot \mid \tau, \boldsymbol{\theta}^{(t-1)}).$$

That is, the optimal density is the conditional density of the latent variables given the data τ and the parameter $\boldsymbol{\theta}^{(t-1)}$. The second optimization problem can be simplified by writing $\mathcal{L}(p^{(t)}, \boldsymbol{\theta}) = Q^{(t)}(\boldsymbol{\theta}) - \mathbb{E}_{p^{(t)}} \ln p^{(t)}(\boldsymbol{Z})$, where

$$Q^{(t)}(\boldsymbol{\theta}) := \mathbb{E}_{p^{(t)}} \ln g(\tau, \boldsymbol{Z} \mid \boldsymbol{\theta})$$

is the expected complete-data log-likelihood under $\boldsymbol{Z} \sim p^{(t)}$. Consequently, the maximization of $\mathcal{L}(p^{(t)}, \boldsymbol{\theta})$ with respect to $\boldsymbol{\theta}$ is equivalent to finding

$$\boldsymbol{\theta}^{(t)} = \operatorname*{argmax}_{\boldsymbol{\theta} \in \Theta} Q^{(t)}(\boldsymbol{\theta}).$$

This leads to the following generic EM algorithm.

Algorithm 4.3.1: Generic EM Algorithm

input: Data τ, initial guess $\boldsymbol{\theta}^{(0)}$.
output: Approximation of the maximum likelihood estimate.

$t \leftarrow 1$
while a stopping criterion is not met **do**
  Expectation Step: Find $p^{(t)}(z) := g(z \mid \tau, \boldsymbol{\theta}^{(t-1)})$ and compute the expectation

$$Q^{(t)}(\boldsymbol{\theta}) := \mathbb{E}_{p^{(t)}} \ln g(\tau, \boldsymbol{Z} \mid \boldsymbol{\theta}). \tag{4.24}$$

  Maximization Step: Let $\boldsymbol{\theta}^{(t)} \leftarrow \operatorname{argmax}_{\boldsymbol{\theta} \in \Theta} Q^{(t)}(\boldsymbol{\theta})$.
  $t \leftarrow t + 1$
return $\boldsymbol{\theta}^{(t)}$

A possible stopping criterion is to stop when

$$\left| \frac{\ln g(\tau \mid \boldsymbol{\theta}^{(t)}) - \ln g(\tau \mid \boldsymbol{\theta}^{(t-1)})}{\ln g(\tau \mid \boldsymbol{\theta}^{(t)})} \right| \leqslant \varepsilon$$

for some small tolerance $\varepsilon > 0$.

■ **Remark 4.1 (Properties of the EM Algorithm)** The identity (4.23) can be used to show that the likelihood $g(\tau \mid \boldsymbol{\theta}^{(t)})$ does not decrease with every iteration of the algorithm. This property is one of the strengths of the algorithm. For example, it can be used to debug computer implementations of the EM algorithm: if the likelihood is observed to decrease at any iteration, then one has detected a bug in the program.

The convergence of the sequence $\{\boldsymbol{\theta}^{(t)}\}$ to a global maximum (if it exists) is highly dependent on the initial value $\boldsymbol{\theta}^{(0)}$ and, in many cases, an appropriate choice of $\boldsymbol{\theta}^{(0)}$ may not be clear. Typically, practitioners run the algorithm from different random starting points over Θ, to ascertain empirically that a suitable optimum is achieved. ■

■ **Example 4.2 (Censored Data)** Suppose the lifetime (in years) of a certain type of machine is modeled via a $\mathcal{N}(\mu, \sigma^2)$ distribution. To estimate μ and σ^2, the lifetimes of n (independent) machines are recorded up to c years. Denote these *censored* lifetimes by $x_1, \ldots, x_n$. The $\{x_i\}$ are thus realizations of iid random variables $\{X_i\}$, distributed as $\min\{Y, c\}$, where $Y \sim \mathcal{N}(\mu, \sigma^2)$.

☞ 430

By the law of total probability (see (C.9)), the marginal pdf of each X can be written as:

$$g(x \,|\, \mu, \sigma^2) = \underbrace{\Phi((c-\mu)/\sigma)}_{\mathbb{P}[Y<c]} \; \frac{\varphi_{\sigma^2}(x-\mu)}{\Phi((c-\mu)/\sigma)} \mathbb{1}\{x < c\} \; + \; \underbrace{\overline{\Phi}((c-\mu)/\sigma)}_{\mathbb{P}[Y \geqslant c]} \; \mathbb{1}\{x = c\},$$

where $\varphi_{\sigma^2}(\cdot)$ is the pdf of the $\mathcal{N}(0, \sigma^2)$ distribution, Φ is the cdf of the standard normal distribution, and $\overline{\Phi} := 1 - \Phi$. It follows that the likelihood of the data $\tau = \{x_1, \ldots, x_n\}$ as a function of the parameter $\boldsymbol{\theta} := [\mu, \sigma^2]^\top$ is:

$$g(\tau \,|\, \boldsymbol{\theta}) = \prod_{i:x_i<c} \frac{\exp\left(-\frac{(x_i-\mu)^2}{2\sigma^2}\right)}{\sqrt{2\pi\sigma^2}} \times \prod_{i:x_i=c} \overline{\Phi}((c-\mu)/\sigma).$$

Let n_c be the total number of x_i such that $x_i = c$. Using n_c latent variables $\boldsymbol{z} = [z_1, \ldots, z_{n_c}]^\top$, we can write the joint pdf:

$$g(\tau, \boldsymbol{z} \,|\, \boldsymbol{\theta}) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left(-\frac{\sum_{i:x_i<c}(x_i-\mu)^2}{2\sigma^2} - \frac{\sum_{i=1}^{n_c}(z_i-\mu)^2}{2\sigma^2}\right) \mathbb{1}\left\{\min_i z_i \geqslant c\right\},$$

so that $\int g(\tau, \boldsymbol{z} \,|\, \boldsymbol{\theta}) \, \mathrm{d}\boldsymbol{z} = g(\tau \,|\, \boldsymbol{\theta})$. We can thus apply the EM algorithm to maximize the likelihood, as follows.

For the E(xpectation)-step, we have for a fixed $\boldsymbol{\theta}$:

$$g(\boldsymbol{z} \,|\, \tau, \boldsymbol{\theta}) = \prod_{i=1}^{n_c} g(z_i \,|\, \tau, \boldsymbol{\theta}),$$

where $g(z \,|\, \tau, \boldsymbol{\theta}) = \mathbb{1}\{z \geqslant c\} \, \varphi_{\sigma^2}(z-\mu)/\overline{\Phi}((c-\mu)/\sigma)$ is simply the pdf of the $\mathcal{N}(\mu, \sigma^2)$ distribution, truncated to $[c, \infty)$.

For the M(aximization)-step, we compute the expectation of the complete log-likelihood with respect to a fixed $g(\boldsymbol{z} \,|\, \tau, \boldsymbol{\theta})$ and use the fact that $Z_1, \ldots, Z_{n_c}$ are iid:

$$\mathbb{E} \ln g(\tau, \boldsymbol{Z} \,|\, \boldsymbol{\theta}) = -\frac{\sum_{i:x_i<c}(x_i-\mu)^2}{2\sigma^2} - \frac{n_c \mathbb{E}(Z-\mu)^2}{2\sigma^2} - \frac{n}{2} \ln \sigma^2 - \frac{n}{2} \ln(2\pi),$$

where Z has a $\mathcal{N}(\mu, \sigma^2)$ distribution, truncated to $[c, \infty)$. To maximize the last expression with respect to μ we set the derivative with respect to μ to zero, and obtain:

$$\mu = \frac{n_c \mathbb{E} Z + \sum_{i:x_i<c} x_i}{n}.$$

Similarly, setting the derivative with respect to σ^2 to zero gives:

$$\sigma^2 = \frac{n_c \mathbb{E}(Z-\mu)^2 + \sum_{i:x_i<c}(x_i-\mu)^2}{n}.$$

In summary, the EM iterates for $t = 1, 2, \ldots$ are as follows.

E-step. Given the current estimate $\boldsymbol{\theta}_t := [\mu_t, \sigma_t^2]^\top$, compute the expectations $\nu_t := \mathbb{E}Z$ and $\zeta_t^2 := \mathbb{E}(Z - \mu_t)^2$, where $Z \sim \mathcal{N}(\mu_t, \sigma_t^2)$, conditional on $Z \geqslant c$; that is,

$$\nu_t := \mu_t + \sigma_t^2 \frac{\varphi_{\sigma_t^2}(c - \mu_t)}{\overline{\Phi}((c - \mu_t)/\sigma_t)}$$
$$\zeta_t^2 := \sigma_t^2 \left(1 + (c - \mu_t) \frac{\varphi_{\sigma_t^2}(c - \mu_t)}{\overline{\Phi}((c - \mu_t)/\sigma_t)}\right).$$

M-step. Update the estimate to $\boldsymbol{\theta}_{t+1} := [\mu_{t+1}, \sigma_{t+1}^2]^\top$ via the formulas:

$$\mu_{t+1} = \frac{n_c \nu_t + \sum_{i:x_i<c} x_i}{n}$$
$$\sigma_{t+1}^2 = \frac{n_c \zeta_t^2 + \sum_{i:x_i<c} (x_i - \mu_{t+1})^2}{n}.$$

■

4.4 Empirical Distribution and Density Estimation

In Section 1.5.2.3 we saw how the empirical cdf $\widehat{F}_n$, obtained from an iid training set $\tau = \{x_1, \ldots, x_n\}$ from an unknown distribution on $\mathbb{R}$, gives an estimate of the unknown cdf F of this sampling distribution. The function $\widehat{F}_n$ is a genuine cdf, as it is right-continuous, increasing, and lies between 0 and 1. The corresponding discrete probability distribution is called the *empirical distribution* of the data. A random variable X distributed according to this empirical distribution takes the values $x_1, \ldots, x_n$ with equal probability $1/n$. The concept of empirical distribution naturally generalizes to higher dimensions: a random vector $\boldsymbol{X}$ that is distributed according to the empirical distribution of $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ has discrete pdf $\mathbb{P}[\boldsymbol{X} = \boldsymbol{x}_i] = 1/n, i = 1, \ldots, n$. Sampling from such a distribution — in other words *resampling* the original data — was discussed in Section 3.2.4. The preeminent usage of such sampling is the bootstrap method, discussed in Section 3.3.2.

☞ 11

EMPIRICAL DISTRIBUTION

☞ 76
☞ 88

In a way, the empirical distribution is the natural answer to the unsupervised learning question: what is the underlying probability distribution of the data? However, the empirical distribution is, by definition, a discrete distribution, whereas the true sampling distribution might be continuous. For continuous data it makes sense to also consider estimation of the pdf of the data. A common approach is to estimate the density via a *kernel density estimate* (KDE), the most prevalent learner to carry this out is given next.

Definition 4.1: Gaussian KDE

Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^d$ be the outcomes of an iid sample from a continuous pdf f. A *Gaussian kernel density estimate* of f is a mixture of normal pdfs, of the form

$$g_{\tau_n}(\boldsymbol{x} \,|\, \sigma) = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{(2\pi)^{d/2} \sigma^d} \, \mathrm{e}^{-\frac{\|\boldsymbol{x} - \boldsymbol{x}_i\|^2}{2\sigma^2}}, \quad \boldsymbol{x} \in \mathbb{R}^d, \tag{4.25}$$

where $\sigma > 0$ is called the *bandwidth*.

GAUSSIAN KERNEL DENSITY ESTIMATE

We see that g_{τ_n} in (4.25) is the average of a collection of n normal pdfs, where each normal distribution is centered at the data point $\boldsymbol{x}_i$ and has covariance matrix $\sigma^2 \mathbf{I}_d$. A major question is how to choose the bandwidth σ so as to best approximate the unknown pdf f. Choosing very small σ will result in a "spiky" estimate, whereas a large σ will produce an over-smoothed estimate that may not identify important peaks that are present in the unknown pdf. Figure 4.1 illustrates this phenomenon. In this case the data are comprised of 20 points uniformly drawn from the unit square. The true pdf is thus 1 on $[0,1]^2$ and 0 elsewhere.

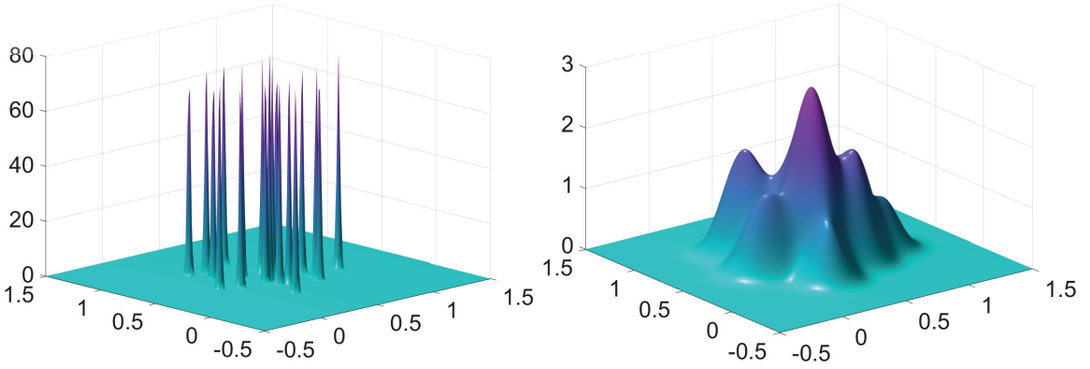


Figure 4.1: Two two-dimensional Gaussian KDEs, with $\sigma = 0.01$ (left) and $\sigma = 0.1$ (right).

Let us write the Gaussian KDE in (4.25) as

$$g_{\tau_n}(\boldsymbol{x} \,|\, \sigma) = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\sigma^d} \phi\left(\frac{\boldsymbol{x} - \boldsymbol{x}_i}{\sigma}\right), \tag{4.26}$$

where

$$\phi(\boldsymbol{z}) = \frac{1}{(2\pi)^{d/2}} \, \mathrm{e}^{-\frac{\|\boldsymbol{z}\|^2}{2}}, \quad \boldsymbol{z} \in \mathbb{R}^d \tag{4.27}$$

is the pdf of the d-dimensional standard normal distribution. By choosing a different probability density ϕ in (4.26), satisfying $\phi(\boldsymbol{x}) = \phi(-\boldsymbol{x})$ for all $\boldsymbol{x}$, we can obtain a wide variety of kernel density estimates. A simple pdf ϕ is, for example, the uniform pdf on $[-1,1]^d$:

$$\phi(\boldsymbol{z}) = \begin{cases} 2^{-d}, & \text{if } \boldsymbol{z} \in [-1,1]^d, \\ 0, & \text{otherwise.} \end{cases}$$

Figure 4.2 shows the graph of the corresponding KDE, using the same data as in Figure 4.1 and with bandwidth $\sigma = 0.1$. We observe qualitatively similar behavior for the Gaussian and uniform KDEs. As a rule, the choice of the function ϕ is less important than the choice of the bandwidth in determining the quality of the estimate.

The important issue of bandwidth selection has been extensively studied for one-dimensional data. To explain the ideas, we use our usual setup and let $\tau = \{x_1, \ldots, x_n\}$ be the observed (one-dimensional) data from the unknown pdf f. First, we define the loss function as

$$\mathrm{Loss}(f(x), g(x)) = \frac{(f(x) - g(x))^2}{f(x)}. \tag{4.28}$$

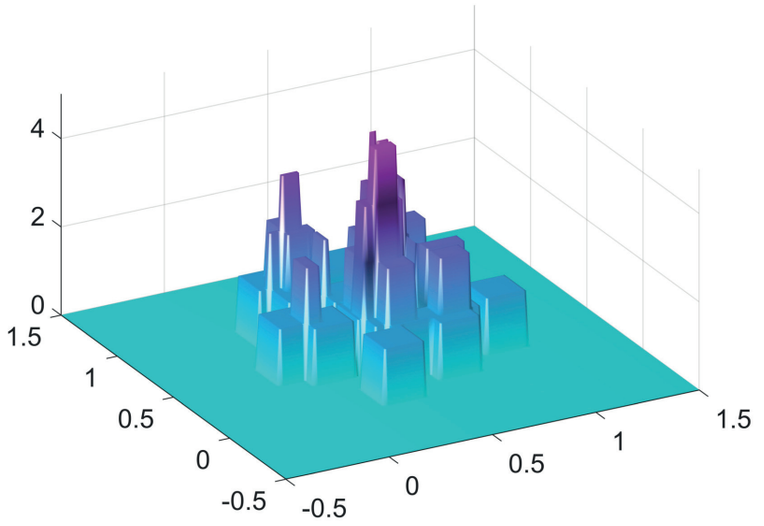


Figure 4.2: A two-dimensional uniform KDE, with bandwidth $\sigma = 0.1$.

The risk to minimize is thus $\ell(g) := \mathbb{E}_f \text{Loss}(f(X), g(X)) = \int (f(x) - g(x))^2 \, \mathrm{d}x$. We bypass the selection of a class of approximation functions by choosing the learner to be specified by (4.25) for a fixed σ. The objective is now to find a σ that minimizes the generalization risk $\ell(g_\tau(\cdot \,|\, \sigma))$ or the expected generalization risk $\mathbb{E}\ell(g_{\mathcal{T}}(\cdot \,|\, \sigma))$. The generalization risk is in this case

$$\int (f(x) - g_\tau(x \,|\, \sigma))^2 \, \mathrm{d}x = \int f^2(x) \, \mathrm{d}x - 2 \int f(x) g_\tau(x \,|\, \sigma) \, \mathrm{d}x + \int g_\tau^2(x \,|\, \sigma) \, \mathrm{d}x.$$

Minimizing this expression with respect to σ is equivalent to minimizing the last two terms, which can be written as

$$-2 \, \mathbb{E}_f g_\tau(X \,|\, \sigma) + \int \left(\frac{1}{n} \sum_{i=1}^{n} \frac{1}{\sigma} \phi\left(\frac{x - x_i}{\sigma} \right) \right)^2 \mathrm{d}x.$$

This expression in turn can be estimated by using a test sample $\{x'_1 \ldots, x'_{n'}\}$ from f, yielding the following minimization problem:

$$\min_\sigma -\frac{2}{n'} \sum_{i=1}^{n'} g_\tau(x'_i \,|\, \sigma) + \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \int \frac{1}{\sigma^2} \phi\left(\frac{x - x_i}{\sigma} \right) \phi\left(\frac{x - x_j}{\sigma} \right) \mathrm{d}x,$$

where $\int \frac{1}{\sigma^2} \phi\left(\frac{x - x_i}{\sigma} \right) \phi\left(\frac{x - x_j}{\sigma} \right) \mathrm{d}x = \frac{1}{\sqrt{2}\sigma} \phi\left(\frac{x_i - x_j}{\sqrt{2}\sigma} \right)$ in the case of the Gaussian kernel (4.27) with $d = 1$. To estimate σ in this way clearly requires a test sample, or at least an application of *cross-validation*. Another approach is to minimize the *expected* generalization risk, (that is, averaged over all training sets):

☞ 37

$$\mathbb{E} \int (f(x) - g_{\mathcal{T}}(x \,|\, \sigma))^2 \, \mathrm{d}x.$$

This is called the *mean integrated squared error* (MISE). It can be decomposed into an integrated squared bias and integrated variance component:

MEAN INTEGRATED SQUARED ERROR

$$\int (f(x) - \mathbb{E} g_{\mathcal{T}}(x \,|\, \sigma))^2 \, \mathrm{d}x + \int \mathbb{V}\text{ar}(g_{\mathcal{T}}(x \,|\, \sigma)) \, \mathrm{d}x.$$

A typical analysis now proceeds by investigating how the MISE behaves for large n, under various assumptions on f. For example, it is shown in [114] that, for $\sigma \to 0$ and $n\sigma \to \infty$, the asymptotic approximation to the MISE of the Gaussian kernel density estimator (4.25) (for $d = 1$) is given by

$$\frac{1}{4}\,\sigma^4\,\|f''\|^2 + \frac{1}{2n\sqrt{\pi\sigma^2}}, \tag{4.29}$$

where $\|f''\|^2 := \int (f''(x))^2\,\mathrm{d}x$. The asymptotically optimal value of σ is the minimizer

$$\sigma^* := \left(\frac{1}{2n\sqrt{\pi}\,\|f''\|^2}\right)^{1/5}. \tag{4.30}$$

GAUSSIAN RULE OF THUMB

To compute the optimal σ^* in (4.30), one needs to estimate the functional $\|f''\|^2$. The *Gaussian rule of thumb* is to assume that f is the density of the $\mathcal{N}(\bar{x}, s^2)$ distribution, where $\bar{x}$ and s^2 are the sample mean and variance of the data, respectively [113]. In this case $\|f''\|^2 = s^{-5}\pi^{-1/2}3/8$ and the Gaussian rule of thumb becomes:

$$\sigma_{\text{rot}} = \left(\frac{4\,s^5}{3\,n}\right)^{1/5} \approx 1.06\; s\, n^{-1/5}.$$

THETA KDE

We recommend, however, the fast and reliable *theta KDE* of [14], which chooses the bandwidth in an optimal way via a fixed-point procedure. Figures 4.1 and 4.2 illustrate a common problem with traditional KDEs: for distributions on a bounded domain, such as the uniform distribution on $[0, 1]^2$, the KDE assigns positive probability mass *outside* this domain. An additional advantage of the theta KDE is that it largely avoids this boundary effect. We illustrate the theta KDE with the following example.

■ **Example 4.3 (Comparison of Gaussian and theta KDEs)** The following Python program draws an iid sample from the Exp(1) distribution and constructs a Gaussian kernel density estimate. We see in Figure 4.3 that with an appropriate choice of the bandwidth a good fit to the true pdf can be achieved, except at the boundary $x = 0$. The theta KDE does not exhibit this boundary effect. Moreover, it chooses the bandwidth automatically, to achieve a superior fit. The theta KDE source code is available as `kde.py` on the book's GitHub site.

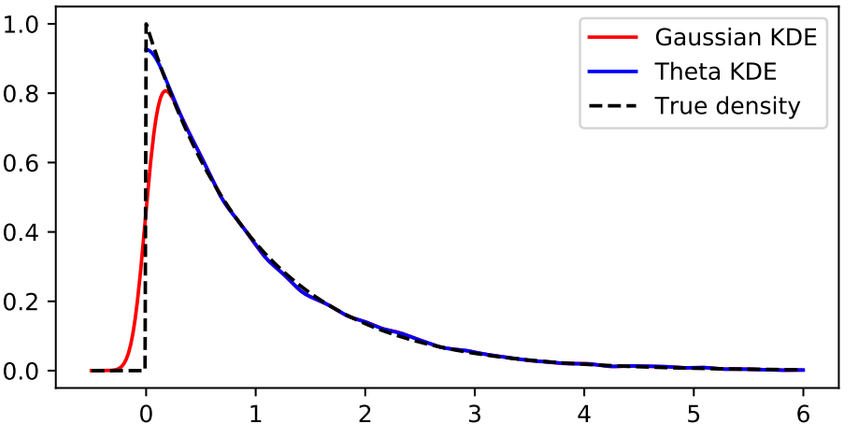


Figure 4.3: Kernel density estimates for Exp(1)-distributed data.

gausthetakde.py

```
import matplotlib.pyplot as plt
import numpy as np
from kde import *

sig = 0.1; sig2 = sig**2; c = 1/np.sqrt(2*np.pi)/sig #Constants
phi = lambda x,x0: np.exp(-(x-x0)**2/(2*sig2)) #Unscaled Kernel
f = lambda x: np.exp(-x)*(x >= 0) # True PDF
n = 10**4 # Sample Size
x = -np.log(np.random.uniform(size=n))# Generate Data via IT method
xx = np.arange(-0.5,6,0.01, dtype = "d")# Plot Range
phis = np.zeros(len(xx))
for i in range(0,n):
    phis = phis + phi(xx,x[i])
phis = c*phis/n
plt.plot(xx,phis,'r')# Plot Gaussian KDE
[bandwidth,density,xmesh,cdf] = kde(x,2**12,0,max(x))
idx = (xmesh <= 6)
plt.plot(xmesh[idx],density[idx])# Plot Theta KDE
plt.plot(xx,f(xx))# Plot True PDF
```

4.5 Clustering via Mixture Models

Clustering is concerned with the grouping of unlabeled feature vectors into clusters, such that samples within a cluster are more similar to each other than samples belonging to different clusters. Usually, it is assumed that the number of clusters is known in advance, but otherwise no prior information is given about the data. Applications of clustering can be found in the areas of communication, data compression and storage, database searching, pattern matching, and object recognition.

A common approach to clustering analysis is to assume that the data comes from a mixture of (usually Gaussian) distributions, and thus the objective is to estimate the parameters of the mixture model by maximizing the likelihood function for the data. Direct optimization of the likelihood function in this case is not a simple task, due to necessary constraints on the parameters (more about this later) and the complicated nature of the likelihood function, which in general has a great number of local maxima and saddle-points. A popular method to estimate the parameters of the mixture model is the EM algorithm, which was discussed in a more general setting in Section 4.3. In this section we explain the basics of mixture modeling and explain the workings of the EM method in this context. In addition, we show how direct optimization methods can be used to maximize the likelihood.

☞ 128

4.5.1 Mixture Models

Let $\mathcal{T} := \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n\}$ be iid random vectors taking values in some set $\mathcal{X} \subseteq \mathbb{R}^d$, each $\boldsymbol{X}_i$ being distributed according to the *mixture density*

MIXTURE DENSITY

$$g(\boldsymbol{x} \,|\, \boldsymbol{\theta}) = w_1 \phi_1(\boldsymbol{x}) + \cdots + w_K \phi_K(\boldsymbol{x}), \quad \boldsymbol{x} \in \mathcal{X}, \tag{4.31}$$

WEIGHTS

where $\phi_1, \ldots, \phi_K$ are probability densities (discrete or continuous) on $\mathcal{X}$, and the positive *weights* $w_1, \ldots, w_K$ sum up to 1. This mixture pdf can be interpreted in the following way. Let Z be a discrete random variable taking values $1, 2, \ldots, K$ with probabilities $w_1, \ldots, w_K$, and let $\boldsymbol{X}$ be a random vector whose conditional pdf, given $Z = z$, is ϕ_z. By the product rule (C.17), the joint pdf of Z and $\boldsymbol{X}$ is given by

☞ 433

$$\phi_{Z,\boldsymbol{X}}(z, \boldsymbol{x}) = \phi_Z(z)\, \phi_{\boldsymbol{X}|Z}(\boldsymbol{x} \,|\, z) = w_z\, \phi_z(\boldsymbol{x})$$

and the marginal pdf of $\boldsymbol{X}$ is found by summing the joint pdf over the values of z, which gives (4.31). A random vector $\boldsymbol{X} \sim g$ can thus be simulated in two steps:

1. First, draw Z according to the probabilities $\mathbb{P}[Z = z] = w_z$, $z = 1, \ldots, K$.
2. Then draw $\boldsymbol{X}$ according to the pdf ϕ_Z.

As $\mathcal{T}$ only contain the $\{\boldsymbol{X}_i\}$ variables, the $\{Z_i\}$ are viewed as *latent* variables. We can interpret Z_i as the hidden label of the cluster to which $\boldsymbol{X}_i$ belongs.

Typically, each ϕ_k in (4.31) is assumed to be known up to some parameter vector $\boldsymbol{\eta}_k$. It is customary[1] in clustering analysis to work with *Gaussian* mixtures; that is, each density ϕ_k is Gaussian with some unknown expectation vector $\boldsymbol{\mu}_k$ and covariance matrix $\boldsymbol{\Sigma}_k$. We gather all unknown parameters, including the weights $\{w_k\}$, into a parameter vector $\boldsymbol{\theta}$. As usual, $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ denotes the outcome of $\mathcal{T}$. As the components of $\mathcal{T}$ are iid, their (joint) pdf is given by

$$g(\tau \,|\, \boldsymbol{\theta}) := \prod_{i=1}^{n} g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}) = \prod_{i=1}^{n} \sum_{k=1}^{K} w_k\, \phi_k(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k). \tag{4.32}$$

Following the same reasoning as for (4.5), we can estimate $\boldsymbol{\theta}$ from an outcome τ by maximizing the log-likelihood function

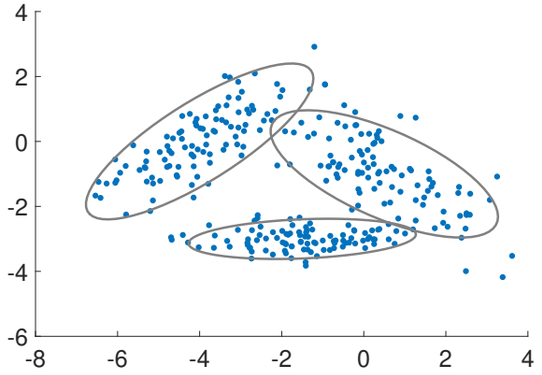
$$l(\boldsymbol{\theta} \,|\, \tau) := \sum_{i=1}^{n} \ln g(\boldsymbol{x}_i \,|\, \boldsymbol{\theta}) = \sum_{i=1}^{n} \ln \left(\sum_{k=1}^{K} w_k\, \phi_k(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) \right). \tag{4.33}$$

However, finding the maximizer of $l(\boldsymbol{\theta} \,|\, \tau)$ is not easy in general, since the function is typically multiextremal.

■ **Example 4.4 (Clustering via Mixture Models)** The data depicted in Figure 4.4 consists of 300 data points that were independently generated from three bivariate normal distributions, whose parameters are given in that same figure. For each of these three distributions, exactly 100 points were generated. Ideally, we would like to cluster the data into three clusters that correspond to the three cases.

To cluster the data into three groups, a possible model for the data is to assume that the points are iid draws from an (unknown) mixture of three 2-dimensional Gaussian distributions. This is a sensible approach, although in reality the data were not simulated in this way. It is instructive to understand the difference between the two models. In the mixture model, each cluster label Z takes the value $\{1, 2, 3\}$ with equal probability, and hence, drawing the labels independently, the total number of points in each cluster would

[1] Other common mixture distributions include Student t and Beta distributions.



cluster	mean vector	covariance matrix
1	$\begin{bmatrix} -4 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 1.4 \\ 1.4 & 1.5 \end{bmatrix}$
2	$\begin{bmatrix} 0.5 \\ -1 \end{bmatrix}$	$\begin{bmatrix} 2 & -0.95 \\ -0.95 & 1 \end{bmatrix}$
3	$\begin{bmatrix} -1.5 \\ -3 \end{bmatrix}$	$\begin{bmatrix} 2 & 0.1 \\ 0.1 & 0.1 \end{bmatrix}$

Figure 4.4: Cluster the 300 data points (left) into three clusters, without making any assumptions about the probability distribution of the data. In fact, the data were generated from three bivariate normal distributions, whose parameters are listed on the right.

be $\mathsf{Bin}(300, 1/3)$ distributed. However, in the actual simulation, the number of points in each cluster is exactly 100. Nevertheless, the mixture model would be an accurate (although not exact) model for these data. Figure 4.5 displays the "target" Gaussian mixture density for the data in Figure 4.4; that is, the mixture with equal weights and with the exact parameters as specified in Figure 4.4.

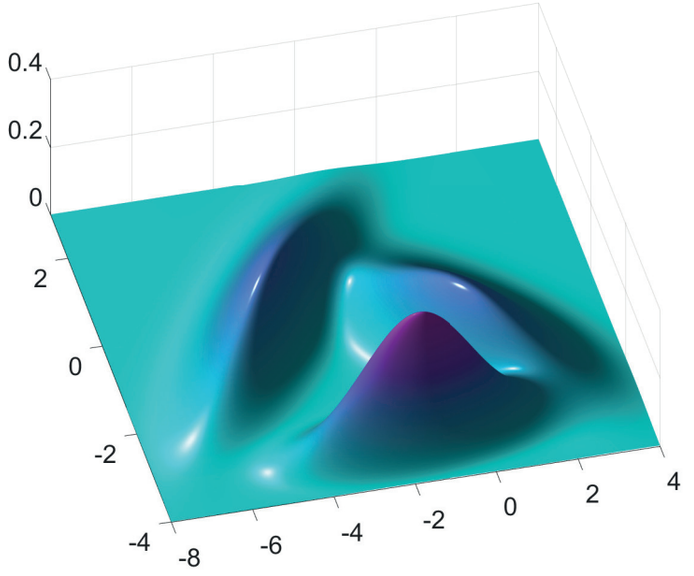


Figure 4.5: The target mixture density for the data in Figure 4.4.

In the next section we will carry out the clustering by using the EM algorithm. ■

4.5.2 EM Algorithm for Mixture Models

As we saw in Section 4.3, instead of maximizing the log-likelihood function (4.33) directly from the data $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, the EM algorithm first *augments* the data with the vector of latent variables — in this case the hidden cluster labels $\boldsymbol{z} = \{z_1, \ldots, z_n\}$. The idea is that τ is

DATA AUGMENTATION

only the *observed* part of the complete random data $(\mathcal{T}, \boldsymbol{Z})$, which were generated via the two-step procedure described above. That is, for each data point $\boldsymbol{X}$, first draw the cluster label $Z \in \{1, \ldots, K\}$ according to probabilities $\{w_1, \ldots, w_K\}$ and then, given $Z = z$, draw $\boldsymbol{X}$ from ϕ_z. The joint pdf of $\mathcal{T}$ and $\boldsymbol{Z}$ is

$$g(\tau, z \,|\, \boldsymbol{\theta}) = \prod_{i=1}^{n} w_{z_i}\, \phi_{z_i}(\boldsymbol{x}_i),$$

which is of a much simpler form than (4.32). It follows that the *complete-data log-likelihood* function

COMPLETE-DATA LOG-LIKELIHOOD

$$\widetilde{l}(\boldsymbol{\theta} \,|\, \tau, z) = \sum_{i=1}^{n} \ln[w_{z_i}\, \phi_{z_i}(\boldsymbol{x}_i)] \tag{4.34}$$

is often easier to maximize than the original log-likelihood (4.33), for any given (τ, z). But, of course the latent variables z are not observed and so $\widetilde{l}(\boldsymbol{\theta} \,|\, \tau, z)$ cannot be evaluated. In the E-step of the EM algorithm, the complete-data log-likelihood is replaced with the expectation $\mathbb{E}_p\, \widetilde{l}(\boldsymbol{\theta} \,|\, \tau, \boldsymbol{Z})$, where the subscript p in the expectation indicates that $\boldsymbol{Z}$ is distributed according to the conditional pdf of $\boldsymbol{Z}$ given $\mathcal{T} = \tau$; that is, with pdf

$$p(z) = g(z \,|\, \tau, \boldsymbol{\theta}) \propto g(\tau, z \,|\, \boldsymbol{\theta}). \tag{4.35}$$

Note that $p(z)$ is of the form $p_1(z_1) \cdots p_n(z_n)$ so that, given $\mathcal{T} = \tau$, the components of $\boldsymbol{Z}$ are independent of each other. The EM algorithm for mixture models can now be formulated as follows.

Algorithm 4.5.1: EM Algorithm for Mixture Models

input: Data τ, initial guess $\boldsymbol{\theta}^{(0)}$.
output: Approximation of the maximum likelihood estimate.

$t \leftarrow 1$
while a stopping criterion is not met **do**
  Expectation Step: Find $p^{(t)}(z) := g(z \,|\, \tau, \boldsymbol{\theta}^{(t-1)})$ and $Q^{(t)}(\boldsymbol{\theta}) := \mathbb{E}_{p^{(t)}} \widetilde{l}(\boldsymbol{\theta} \,|\, \tau, \boldsymbol{Z})$.
  Maximization Step: Let $\boldsymbol{\theta}^{(t)} \leftarrow \operatorname{argmax}_{\boldsymbol{\theta}} Q^{(t)}(\boldsymbol{\theta})$.
  $t \leftarrow t + 1$
return $\boldsymbol{\theta}^{(t)}$

A possible termination condition is to stop when $\left|l(\boldsymbol{\theta}^{(t)} \,|\, \tau) - l(\boldsymbol{\theta}^{(t-1)} \,|\, \tau)\right| / \left|l(\boldsymbol{\theta}^{(t)} \,|\, \tau)\right| < \varepsilon$ for some small tolerance $\varepsilon > 0$. As was mentioned in Section 4.3, the sequence of log-likelihood values *does not decrease* with each iteration. Under certain continuity conditions, the sequence $\{\boldsymbol{\theta}^{(t)}\}$ is guaranteed to converge to a local maximizer of the log-likelihood l. Convergence to a global maximizer (if it exists) depends on the appropriate choice for the starting value. Typically, the algorithm is run from different random starting points.

For the case of Gaussian mixtures, each $\phi_k = \phi(\cdot \,|\, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k), k = 1, \ldots, K$ is the density of a d-dimensional Gaussian distribution. Let $\boldsymbol{\theta}^{(t-1)}$ be the current guess for the optimal parameter vector, consisting of the weights $\{w_k^{(t-1)}\}$, mean vectors $\{\boldsymbol{\mu}_k^{(t-1)}\}$, and covariance matrices $\{\boldsymbol{\Sigma}_k^{(t-1)}\}$. We first determine $p^{(t)}$ — the pdf of $\boldsymbol{Z}$ conditional on $\mathcal{T} = \tau$ — for the given guess $\boldsymbol{\theta}^{(t-1)}$. As mentioned before, the components of $\boldsymbol{Z}$ given $\mathcal{T} = \tau$ are independent,

so it suffices to specify the discrete pdf, $p_i^{(t)}$ say, of each Z_i given the observed point $\boldsymbol{X}_i = \boldsymbol{x}_i$. The latter can be found from Bayes' formula:

$$p_i^{(t)}(k) \propto w_k^{(t-1)}\, \phi_k(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_k^{(t-1)}, \boldsymbol{\Sigma}_k^{(t-1)}), \quad k = 1, \ldots, K. \tag{4.36}$$

Next, in view of (4.34), the function $Q^{(t)}(\boldsymbol{\theta})$ can be written as

$$Q^{(t)}(\boldsymbol{\theta}) = \mathbb{E}_{p^{(t)}} \sum_{i=1}^{n} \left(\ln w_{Z_i} + \ln\, \phi_{Z_i}(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_{Z_i}, \boldsymbol{\Sigma}_{Z_i}) \right) = \sum_{i=1}^{n} \mathbb{E}_{p_i^{(t)}} \left[\ln w_{Z_i} + \ln\, \phi_{Z_i}(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_{Z_i}, \boldsymbol{\Sigma}_{Z_i}) \right],$$

where the $\{Z_i\}$ are independent and Z_i is distributed according to $p_i^{(t)}$ in (4.36). This completes the *E-step*. In the *M-step* we maximize $Q^{(t)}$ with respect to the parameter $\boldsymbol{\theta}$; that is, with respect to the $\{w_k\}$, $\{\boldsymbol{\mu}_k\}$, and $\{\boldsymbol{\Sigma}_k\}$. In particular, we maximize

$$\sum_{i=1}^{n} \sum_{k=1}^{K} p_i^{(t)}(k) \left[\ln w_k + \ln \phi_k(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k) \right],$$

under the condition $\sum_k w_k = 1$. Using Lagrange multipliers and the fact that $\sum_{k=1}^{K} p_i^{(t)}(k) = 1$ gives the solution for the $\{w_k\}$:

$$w_k = \frac{1}{n} \sum_{i=1}^{n} p_i^{(t)}(k), \quad k = 1, \ldots, K. \tag{4.37}$$

The solutions for $\boldsymbol{\mu}_k$ and $\boldsymbol{\Sigma}_k$ now follow from maximizing $\sum_{i=1}^{n} p_i^{(t)}(k)\, \ln \phi_k(\boldsymbol{x}_i \,|\, \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)$, leading to

$$\boldsymbol{\mu}_k = \frac{\sum_{i=1}^{n} p_i^{(t)}(k)\, \boldsymbol{x}_i}{\sum_{i=1}^{n} p_i^{(t)}(k)}, \quad k = 1, \ldots, K \tag{4.38}$$

and

$$\boldsymbol{\Sigma}_k = \frac{\sum_{i=1}^{n} p_i^{(t)}(k)\, (\boldsymbol{x}_i - \boldsymbol{\mu}_k)(\boldsymbol{x}_i - \boldsymbol{\mu}_k)^\top}{\sum_{i=1}^{n} p_i^{(t)}(k)}, \quad k = 1, \ldots, K, \tag{4.39}$$

which are very similar to the well-known formulas for the MLEs of the parameters of a Gaussian distribution. After assigning the solution parameters to $\boldsymbol{\theta}^{(t)}$ and increasing the iteration counter t by 1, the steps (4.36), (4.37), (4.38), and (4.39) are repeated until convergence is reached. Convergence of the EM algorithm is very sensitive to the choice of initial parameters. It is therefore recommended to try various different starting conditions. For a further discussion of the theoretical and practical aspects of the EM algorithm we refer to [85].

■ **Example 4.5 (Clustering via EM)** We return to the data in Example 4.4, depicted in Figure 4.4, and adopt the model that the data is coming from a mixture of three bivariate Gaussian distributions.

The Python code below implements the EM procedure described in Algorithm 4.5.1. The initial mean vectors $\{\boldsymbol{\mu}_k\}$ of the bivariate Gaussian distributions are chosen (from visual inspection) to lie roughly in the middle of each cluster, in this case $[-2, -3]^\top$, $[-4, 1]^\top$, and $[0, -1]^\top$. The corresponding covariance matrices are initially chosen as identity matrices, which is appropriate given the observed spread of the data in Figure 4.4. Finally, the initial weights are $1/3, 1/3, 1/3$. For simplicity, the algorithm stops after 100 iterations, which in this case is more than enough to guarantee convergence. The code and data are available from the book's website in the GitHub folder Chapter4.

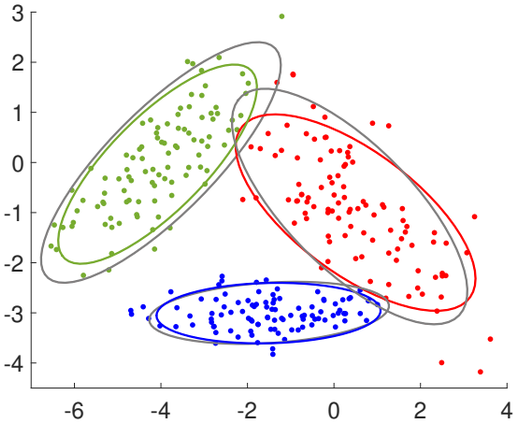
EMclust.py

```
import numpy as np
from scipy.stats import multivariate_normal

Xmat = np.genfromtxt('clusterdata.csv', delimiter=',')
K = 3
n, D = Xmat.shape

W = np.array([[1/3,1/3,1/3]])
M  = np.array([[-2.0,-4,0],[-3,1,-1]], dtype=np.float32)
# Note that if above *all* entries were written as integers, M would
# be defined to be of integer type, which will give the wrong answer

C = np.zeros((3,2,2))

C[:,0,0] = 1
C[:,1,1] = 1

p = np.zeros((3,300))

for i in range(0,100):

#E-step
    for k in range(0,K):
        mvn = multivariate_normal( M[:,k].T, C[k,:,:] )
        p[k,:] = W[0,k]*mvn.pdf(Xmat)

# M-Step
    p = (p/sum(p,0))   #normalize
    W = np.mean(p,1).reshape(1,3)

    for k in range(0,K):
        M[:,k] = (Xmat.T @ p[k,:].T)/sum(p[k,:])
        xm = Xmat.T - M[:,k].reshape(2,1)
        C[k,:,:] = xm @ (xm*p[k,:]).T/sum(p[k,:])
```

The estimated parameters of the mixture distribution are given on the right-hand side of Figure 4.6. After relabeling of the clusters, we can observe a close match with the parameters in Figure 4.4.

The ellipses on the left-hand side of Figure 4.6 show a close match between the 95% probability ellipses[2] of the original Gaussian distributions (in gray) and the estimated ones. A natural way to cluster each point $\boldsymbol{x}_i$ is to assign it to the cluster k for which the conditional probability $p_i(k)$ is maximal (with ties resolved arbitrarily). This gives the clustering of the points into red, green, and blue clusters in the figure.

[2]For each mixture component, the contour of the corresponding bivariate normal pdf is shown that encloses 95% of the probability mass.



weight	mean vector	covariance matrix
0.33	$\begin{bmatrix}-1.51\\-3.01\end{bmatrix}$	$\begin{bmatrix}1.75 & 0.03\\0.03 & 0.095\end{bmatrix}$
0.32	$\begin{bmatrix}-4.08\\-0.033\end{bmatrix}$	$\begin{bmatrix}1.37 & 0.92\\0.92 & 1.03\end{bmatrix}$
0.35	$\begin{bmatrix}0.36\\-0.88\end{bmatrix}$	$\begin{bmatrix}1.93 & -1.20\\-1.20 & 1.44\end{bmatrix}$

Figure 4.6: The results of the EM clustering algorithm applied to the data depicted in Figure 4.4.

As an alternative to the EM algorithm, one can of course use continuous multiextremal optimization algorithms to directly optimize the log-likelihood function $l(\boldsymbol{\theta}\,|\,\tau) = \ln g(\tau\,|\,\boldsymbol{\theta})$ in (4.33) over the set Θ of all possible $\boldsymbol{\theta}$. This is done for example in [15], demonstrating superior results to EM when there are few data points. Closer investigation of the likelihood function reveals that there is a hidden problem with any maximum likelihood approach for clustering if Θ is chosen as large as possible — i.e., any mixture distribution is possible. To demonstrate this problem, consider Figure 4.7, depicting the probability density function, $g(\cdot\,|\,\boldsymbol{\theta})$ of a mixture of two Gaussian distributions, where $\boldsymbol{\theta} = [w, \mu_1, \sigma_1^2, \mu_2, \sigma_2^2]^\top$ is the vector of parameters for the mixture distribution. The log-likelihood function is given by $l(\boldsymbol{\theta}\,|\,\tau) = \sum_{i=1}^{4} \ln g(x_i\,|\,\boldsymbol{\theta})$, where $x_1, \ldots, x_4$ are the data (indicated by dots in the figure).

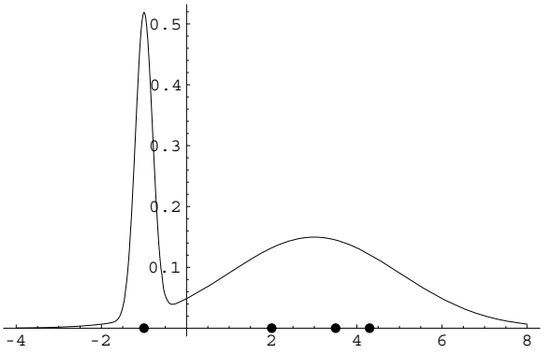


Figure 4.7: Mixture of two Gaussian distributions.

It is clear that by fixing the mixing constant w at 0.25 (say) and centering the first cluster at x_1, one can obtain an arbitrarily large likelihood value by taking the variance of the first cluster to be arbitrarily small. Similarly, for higher dimensional data, by choosing "point" or "line" clusters, or in general "degenerate" clusters, one can make the value of the likelihood infinite. This is a manifestation of the familiar overfitting problem for the

training loss that we already encountered in Chapter 2. Thus, the unconstrained maximization of the log-likelihood function is an ill-posed problem, irrespective of the choice of the optimization algorithm!

Two possible solutions to this "overfitting" problem are:

1. Restrict the parameter set Θ in such a way that degenerate clusters (sometimes called spurious clusters) are not allowed.
2. Run the given algorithm and if the solution is degenerate, discard it and run the algorithm afresh. Keep restarting the algorithm until a non-degenerate solution is obtained.

The first approach is usually applied to multiextremal optimization algorithms and the second is used for the EM algorithm.

4.6 Clustering via Vector Quantization

In the previous section we introduced clustering via mixture models, as a form of parametric density estimation (as opposed to the nonparametric density estimation in Section 4.4). The clusters were modeled in a natural way via the latent variables and the EM algorithm provided a convenient way to assign the cluster members. In this section we consider a more heuristic approach to clustering by ignoring the distributional properties of the data. The resulting algorithms tend to scale better with the number of samples n and the dimensionality d.

In mathematical terms, we consider the following clustering (also called data segmentation) problem. Given a collection $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ of data points in some d-dimensional space $\mathcal{X}$, divide this data set into K clusters (groups) such that some loss function is minimized. A convenient way to determine these clusters is to first divide up the entire space $\mathcal{X}$, using some distance function $\mathrm{dist}(\cdot, \cdot)$ on this space. A standard choice is the Euclidean (or L_2) distance:

$$\mathrm{dist}(\boldsymbol{x}, \boldsymbol{x}') = \|\boldsymbol{x} - \boldsymbol{x}'\| = \sqrt{\sum_{i=1}^{d} (x_i - x_i')^2}.$$

MANHATTAN DISTANCE

Other commonly used distance measures on $\mathbb{R}^d$ include the *Manhattan distance*:

$$\sum_{i=1}^{d} |x_i - x_i'|$$

MAXIMUM DISTANCE

and the *maximum distance*:

$$\max_{i=1,\ldots,d} |x_i - x_i'|.$$

HAMMING DISTANCE

On the set of strings of length d, an often-used distance measure is the *Hamming distance*:

$$\sum_{i=1}^{d} \mathbb{1}\{x_i \neq x_i'\},$$

that is, the number of mismatched characters. For example, the Hamming distance between 010101 and 011010 is 4.

We can partition the space $\mathcal{X}$ into regions as follows: First, we choose K points $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$ called *cluster centers* or *source vectors*. For each $k = 1, \ldots, K$, let

SOURCE VECTORS

$$\mathcal{R}_k = \{\boldsymbol{x} \in \mathcal{X} : \text{dist}(\boldsymbol{x}, \boldsymbol{c}_k) \leqslant \text{dist}(\boldsymbol{x}, \boldsymbol{c}_i) \text{ for all } i \neq k\}$$

be the set of points in $\mathcal{X}$ that lie closer to $\boldsymbol{c}_k$ than any other center. The regions or *cells* $\{\mathcal{R}_k\}$ divide the space $\mathcal{X}$ into what is called a *Voronoi diagram* or a *Voronoi tessellation*. Figure 4.8 shows a Voronoi tessellation of the plane into ten regions, using the Euclidean distance. Note that here the boundaries between the Voronoi cells are straight line segments. In particular, if cell $\mathcal{R}_i$ and $\mathcal{R}_j$ share a border, then a point on this border must satisfy $\|\boldsymbol{x} - \boldsymbol{c}_i\| = \|\boldsymbol{x} - \boldsymbol{c}_j\|$; that is, it must lie on the line that passes through the point $(\boldsymbol{c}_j + \boldsymbol{c}_i)/2$ (that is, the midway point of the line segment between $\boldsymbol{c}_i$ and $\boldsymbol{c}_j$) and be perpendicular to $\boldsymbol{c}_j - \boldsymbol{c}_i$.

VORONOI TESSELLATION

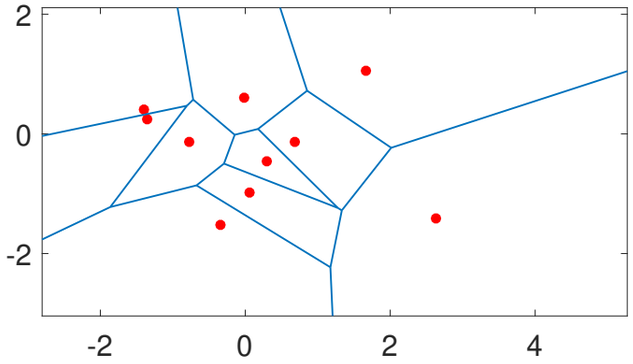


Figure 4.8: A Voronoi tessellation of the plane into ten cells, determined by the (red) centers.

Once the centers (and thus the cells $\{\mathcal{R}_k\}$) are chosen, the points in τ can be clustered according to their nearest center. Points on the boundary have to be treated separately. This is a moot point for continuous data, as generally no data points will lie exactly on the boundary.

The main remaining issue is how to choose the centers so as to cluster the data in some optimal way. In terms of our (unsupervised) learning framework, we wish to approximate a vector $\boldsymbol{x}$ via one of $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$, using a piecewise constant vector-valued function

$$\boldsymbol{g}(\boldsymbol{x} \,|\, \mathbf{C}) := \sum_{k=1}^{K} \boldsymbol{c}_k \, \mathbb{1}\{\boldsymbol{x} \in \mathcal{R}_k\},$$

where $\mathbf{C}$ is the $d \times K$ matrix $[\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K]$. Thus, $\boldsymbol{g}(\boldsymbol{x} \,|\, \mathbf{C}) = \boldsymbol{c}_k$ when $\boldsymbol{x}$ falls in region $\mathcal{R}_k$ (we ignore ties). Within this class $\mathcal{G}$ of functions, parameterized by $\mathbf{C}$, our aim is to minimize the training loss. In particular, for the squared-error loss, $\text{Loss}(\boldsymbol{x}, \boldsymbol{x}') = \|\boldsymbol{x} - \boldsymbol{x}'\|^2$, the training loss is

$$\ell_{\tau_n}(\boldsymbol{g}(\cdot \,|\, \mathbf{C})) = \frac{1}{n} \sum_{i=1}^{n} \|\boldsymbol{x}_i - \boldsymbol{g}(\boldsymbol{x}_i \,|\, \mathbf{C})\|^2 = \frac{1}{n} \sum_{k=1}^{K} \sum_{\boldsymbol{x} \in \mathcal{R}_k \cap \tau_n} \|\boldsymbol{x} - \boldsymbol{c}_k\|^2. \tag{4.40}$$

Thus, the training loss minimizes the average squared distance between the centers. This framework also combines both the encoding and decoding steps in *vector quantization*

VECTOR QUANTIZATION

[125]. Namely, we wish to "quantize" or "encode" the vectors in τ in such a way that each vector is represented by one of K source vectors $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$, such that the loss (4.40) of this representation is minimized.

Most well-known clustering and vector quantization methods update the vector of centers, starting from some initial choice and using iterative (typically gradient-based) procedures. It is important to realize that in this case (4.40) is seen as a function of the centers, where each point $\boldsymbol{x}$ is assigned to the nearest center, thus determining the clusters. It is well known that this type of problem — optimization with respect to the centers — is highly multiextremal and, depending on the initial clusters, gradient-based procedures tend to converge to a *local minimum* rather than a global minimum.

4.6.1 K-Means

CENTROIDS

One of the simplest methods for clustering is the K-means method. It is an iterative method where, starting from an initial guess for the centers, new centers are formed by taking sample means of the current points in each cluster. The new centers are thus the *centroids* of the points in each cell. Although there exist many different varieties of the K-means algorithm, they are all essentially of the following form:

Algorithm 4.6.1: K-Means

input: Collection of points $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, number of clusters K, initial centers $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K$.

output: Cluster centers and cells (regions).

1 **while** a stopping criterion is not met **do**
2 $\quad \mathcal{R}_1, \ldots, \mathcal{R}_K \leftarrow \emptyset$ (empty sets).
3 $\quad$ **for** $i = 1$ **to** n **do**
4 $\quad\quad \boldsymbol{d} \leftarrow [\mathrm{dist}(\boldsymbol{x}_i, \boldsymbol{c}_1), \ldots, \mathrm{dist}(\boldsymbol{x}_i, \boldsymbol{c}_K)]$ `// distances to centers`
5 $\quad\quad k \leftarrow \mathrm{argmin}_j \, d_j$
6 $\quad\quad \mathcal{R}_k \leftarrow \mathcal{R}_k \cup \{\boldsymbol{x}_i\}$ `// assign` $\boldsymbol{x}_i$ `to cluster` k
7 $\quad$ **for** $k = 1$ **to** K **do**
8 $\quad\quad \boldsymbol{c}_k \leftarrow \dfrac{\sum_{\boldsymbol{x} \in \mathcal{R}_k} \boldsymbol{x}}{|\mathcal{R}_k|}$ `// compute the new center as a centroid of points`
9 **return** $\{\boldsymbol{c}_k\}$, $\{\mathcal{R}_k\}$

Thus, at each iteration, for a given choice of centers, each point in τ is assigned to its nearest center. After all points have been assigned, the centers are recomputed as the centroids of all the points in the current cluster (Line 8). A typical stopping criterion is to stop when the centers no longer change very much. As the algorithm is quite sensitive to the choice of the initial centers, it is prudent to try multiple starting values, e.g., chosen randomly from the bounding box of the data points.

We can see the K-means method as a deterministic (or "hard") version of the probabilistic (or "soft") EM algorithm as follows. Suppose in the EM algorithm we have Gaussian mixtures with a fixed covariance matrix $\boldsymbol{\Sigma}_k = \sigma^2 \mathbf{I}_d$, $k = 1, \ldots, K$, where σ^2 should be thought of as being infinitesimally small. Consider iteration t of the EM algorithm. Having obtained the expectation vectors $\boldsymbol{\mu}_k^{(t-1)}$ and weights $w_k^{(t-1)}, k = 1, \ldots, K$, each point $\boldsymbol{x}_i$ is assigned a cluster label Z_i according to the probabilities $p_i^{(t)}(k), k = 1, \ldots, K$ given in (4.36).

But for $\sigma^2 \to 0$ the probability distribution $\{p_i^{(t)}(k)\}$ becomes degenerate, putting all its probability mass on $\operatorname{argmin}_k \|\boldsymbol{x}_i - \boldsymbol{\mu}_k\|^2$. This corresponds to the K-means rule of assigning $\boldsymbol{x}_i$ to its nearest cluster center. Moreover, in the M-step (4.38) each cluster center $\boldsymbol{\mu}_k^{(t)}$ is now updated according to the average of the $\{\boldsymbol{x}_i\}$ that have been assigned to cluster k. We thus obtain the same deterministic updating rule as in K-means.

■ **Example 4.6 (K-means Clustering)** We cluster the data from Figure 4.4 via K-means, using the Python implementation below. Note that the data points are stored as a 300×2 matrix `Xmat`. We take the same starting centers as in the EM example: $\boldsymbol{c}_1 = [-2, -3]^\top$, $\boldsymbol{c}_2 = [-4, 1]^\top$, and $\boldsymbol{c}_3 = [0, -1]^\top$. Note also that *squared* Euclidean distances are used in the computations, as these are slightly faster to compute than Euclidean distances (as no square root computations are required) while yielding exactly the same cluster center evaluations.

Kmeans.py

```
import numpy as np
Xmat = np.genfromtxt('clusterdata.csv', delimiter=',')
K = 3
n, D = Xmat.shape
c  = np.array([[-2.0,-4,0],[-3,1,-1]])  #initialize centers
cold = np.zeros(c.shape)
dist2 = np.zeros((K,n))
while np.abs(c - cold).sum() > 0.001:
   cold = c.copy()
   for i in range(0,K): #compute the squared distances
        dist2[i,:] = np.sum((Xmat - c[:,i].T)**2, 1)

   label = np.argmin(dist2,0) #assign the points to nearest centroid
   minvals = np.amin(dist2,0)
   for i in range(0,K): # recompute the centroids
      c[:,i] = np.mean(Xmat[np.where(label == i),:],1).reshape(1,2)

print('Loss = {:3.3f}'.format(minvals.mean()))
```

```
Loss = 2.288
```

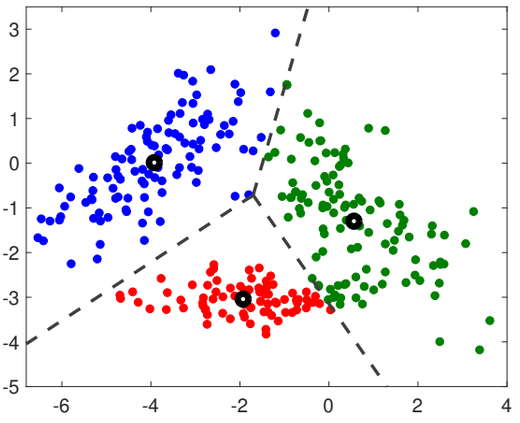


Figure 4.9: Results of the K-means algorithm applied to the data in Figure 4.4. The thick black circles are the centroids and the dotted lines define the cell boundaries.

We found the cluster centers $\boldsymbol{c}_1 = [-1.9286, -3.0416]^\top$, $\boldsymbol{c}_2 = [-3.9237, 0.0131]^\top$, and $\boldsymbol{c}_3 = [0.5611, -1.2980]^\top$, giving the clustering depicted in Figure 4.9. The corresponding loss (4.40) was found to be 2.288. ■

4.6.2 Clustering via Continuous Multiextremal Optimization

As already mentioned, the exact minimization of the loss function (4.40) is difficult to accomplish via standard local search methods such as gradient descent, as the function is highly multimodal. However, nothing is preventing us from using global optimization
☞ 100 methods such as the CE or SCO methods discussed in Sections 3.4.2 and 3.4.3.

■ **Example 4.7 (Clustering via CE)** We take the same data set as in Example 4.6 and cluster the points via minimization of the loss (4.40) using the CE method. The Python
☞ 101 code below is very similar to the code in Example 3.16, except that now we are dealing with a six-dimensional optimization problem. The loss function is implemented in the function `Scluster`, which essentially reuses the squared distance computation of the K-means code in Example 4.6. The CE program typically converges to a loss of 2.287, corresponding to the (global) minimizers $\boldsymbol{c}_1 = [-1.9286, -3.0416]^\top$, $\boldsymbol{c}_2 = [-3.8681, 0.0456]^\top$, and $\boldsymbol{c}_3 = [0.5880, -1.3526]^\top$, which slightly differs from the local minimizers for the K-means algorithm.

clustCE.py

```
import numpy as np
np.set_printoptions(precision=4)

Xmat = np.genfromtxt('clusterdata.csv', delimiter=',')
K = 3
n, D = Xmat.shape

def Scluster(c):
    n, D = Xmat.shape
    dist2 = np.zeros((K,n))
    cc = c.reshape(D,K)
    for i in range(0,K):
        dist2[i,:] = np.sum((Xmat - cc[:,i].T)**2, 1)
    minvals = np.amin(dist2,0)
    return minvals.mean()

numvar = K*D
mu = np.zeros(numvar)  #initialize centers
sigma = np.ones(numvar)*2
rho = 0.1
N = 500; Nel = int(N*rho); eps = 0.001

func = Scluster
best_trj = np.array(numvar)
best_perf = np.Inf
trj = np.zeros(shape=(N,numvar))

while(np.max(sigma)>eps):
   for i in range(0,numvar):
```

```
        trj[:,i] = (np.random.randn(N,1)*sigma[i]+ mu[i]).reshape(N,)
    S = np.zeros(N)
    for i in range(0,N):
        S[i] = func(trj[i])

    sortedids = np.argsort(S) # from smallest to largest
    S_sorted = S[sortedids]
    best_trj = np.array(n)
    best_perf = np.Inf
    eliteids = sortedids[range(0,Nel)]
    eliteTrj = trj[eliteids,:]
    mu = np.mean(eliteTrj,axis=0)
    sigma = np.std(eliteTrj,axis=0)

    if(best_perf>S_sorted[0]):
        best_perf = S_sorted[0]
        best_trj = trj[sortedids[0]]

print(best_perf)
print(best_trj.reshape(2,3))
```

```
2.2874901831572947
[[-3.9238 -1.8477  0.5895]
 [ 0.0134 -3.0292 -1.2442]]
```

4.7 Hierarchical Clustering

It is sometimes useful to determine data clusters in a hierarchical manner; an example is the construction of evolutionary relationships between animal species. Establishing a hierarchy of clusters can be done in a bottom-up or a top-down manner. In the bottom-up approach, also called *agglomerative clustering*, the data points are merged in larger and larger clusters until all the points have been merged into a single cluster. In the top-down or *divisive clustering* approach, the data set is divided up into smaller and smaller clusters. The left panel of Figure 4.10 depicts a hierarchy of clusters.

AGGLOMERATIVE CLUSTERING

DIVISIVE CLUSTERING

In Figure 4.10, each cluster is given a cluster identifier. At the lowest level are clusters comprised of the original data points (identifiers $1, \ldots, 8$). The union of clusters 1 and 2 form a cluster with identifier 9, and the union of 3 and 4 form a cluster with identifier 10. In turn the union of clusters 9 and 10 constitutes cluster 12, and so on.

The right panel of Figure 4.10 shows a convenient way to visualize cluster hierarchies using a *dendrogram* (from the Greek *dendro* for tree). A dendrogram not only summarizes how clusters are merged or split, but also shows the distance between clusters, here on the vertical axis. The horizontal axis shows which cluster each data point (label) belongs to.

DENDROGRAM

Many different types of hierarchical clustering can be performed, depending on how the distance is defined between two data points and between two clusters. Denote the data set by $\mathcal{X} = \{\boldsymbol{x}_i, i = 1, \ldots, n\}$. As in Section 4.6, let $\text{dist}(\boldsymbol{x}_i, \boldsymbol{x}_j)$ be the distance between data points $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$. The default choice is the Euclidean distance $\text{dist}(\boldsymbol{x}_i, \boldsymbol{x}_j) = \|\boldsymbol{x}_i - \boldsymbol{x}_j\|$.

Let $\mathcal{I}$ and $\mathcal{J}$ be two disjoint subsets of $\{1, \ldots, n\}$. These sets correspond to two disjoint subsets (that is, clusters) of $\mathcal{X}$: $\{\boldsymbol{x}_i, i = \mathcal{I}\}$ and $\{\boldsymbol{x}_j, j = \mathcal{J}\}$. We denote the distance between

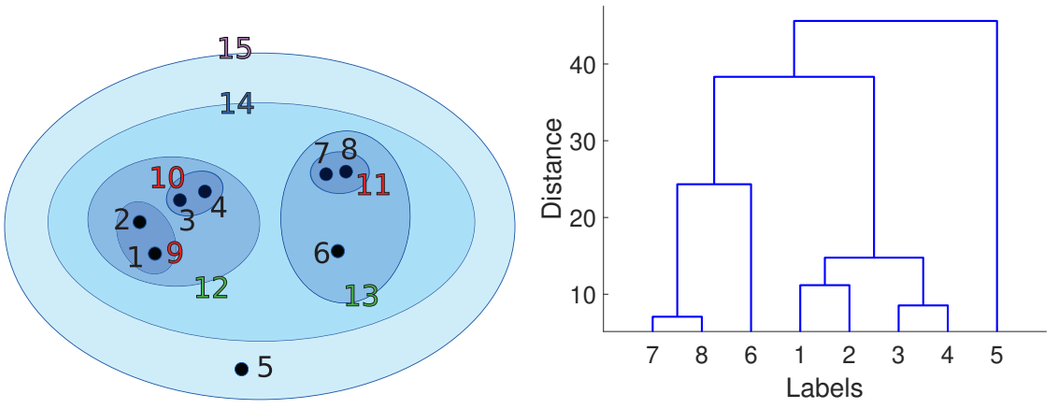


Figure 4.10: Left: a cluster hierarchy of 15 clusters. Right: the corresponding dendrogram.

these two clusters by $d(\mathcal{I}, \mathcal{J})$. By specifying the function d, we indicate how the clusters are linked. For this reason it is also referred to as the *linkage* criterion. We give a number of examples:

LINKAGE

- **Single linkage.** The closest distance between the clusters.

$$d_{\min}(\mathcal{I}, \mathcal{J}) := \min_{i \in \mathcal{I}, j \in \mathcal{J}} \operatorname{dist}(\boldsymbol{x}_i, \boldsymbol{x}_j).$$

- **Complete linkage.** The furthest distance between the clusters.

$$d_{\max}(\mathcal{I}, \mathcal{J}) := \max_{i \in \mathcal{I}, j \in \mathcal{J}} \operatorname{dist}(\boldsymbol{x}_i, \boldsymbol{x}_j).$$

- **Group average.** The mean distance between the clusters. Note that this depends on the cluster sizes.

$$d_{\text{avg}}(\mathcal{I}, \mathcal{J}) := \frac{1}{|\mathcal{I}|\,|\mathcal{J}|} \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} \operatorname{dist}(\boldsymbol{x}_i, \boldsymbol{x}_j).$$

For these linkage criteria, $\mathcal{X}$ is usually assumed to be $\mathbb{R}^d$ with the Euclidean distance.

WARD'S LINKAGE

Another notable measure for the distance between clusters is *Ward's minimum variance linkage* criterion. Here, the distance between clusters is expressed as the additional amount of "variance" (expressed in terms of the sum of squares) that would be introduced if the two clusters were merged. More precisely, for any set $\mathcal{K}$ of indices (labels) let $\overline{\boldsymbol{x}}_{\mathcal{K}} = \sum_{k \in \mathcal{K}} \boldsymbol{x}_k / |\mathcal{K}|$ denote its corresponding cluster mean. Then

$$d_{\text{Ward}}(\mathcal{I}, \mathcal{J}) := \sum_{k \in I \cup \mathcal{J}} \|\boldsymbol{x}_k - \overline{\boldsymbol{x}}_{\mathcal{I} \cup \mathcal{J}}\|^2 - \left(\sum_{i \in \mathcal{I}} \|\boldsymbol{x}_i - \overline{\boldsymbol{x}}_{\mathcal{I}}\|^2 + \sum_{j \in \mathcal{J}} \|\boldsymbol{x}_j - \overline{\boldsymbol{x}}_{\mathcal{J}}\|^2 \right). \tag{4.41}$$

It can be shown (see Exercise 8) that the Ward linkage depends only on the cluster means and the cluster sizes for $\mathcal{I}$ and $\mathcal{J}$:

$$d_{\text{Ward}}(\mathcal{I}, \mathcal{J}) = \frac{|\mathcal{I}|\,|\mathcal{J}|}{|\mathcal{I}| + |\mathcal{J}|} \|\overline{\boldsymbol{x}}_{\mathcal{I}} - \overline{\boldsymbol{x}}_{\mathcal{J}}\|^2.$$

In software implementations, the Ward linkage function is often rescaled by multiplying it by a factor of 2. In this way, the distance between one-point clusters $\{\boldsymbol{x}_i\}$ and $\{\boldsymbol{x}_j\}$ is the *squared* Euclidean distance $\|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2$.

Having chosen a distance on $\mathcal{X}$ and a linkage criterion, a general agglomerative clustering algorithm proceeds in the following "greedy" manner.

Algorithm 4.7.1: Greedy Agglomerative Clustering

input: Distance function dist, linkage function d, number of clusters K.
output: The label sets for the tree.

Initialize the set of cluster identifiers: $\mathcal{I} = \{1, \dots, n\}$.
Initialize the corresponding label sets: $\mathcal{L}_i = \{i\}$, $i \in \mathcal{I}$.
Initialize a distance matrix $\mathbf{D} = [d_{ij}]$ with $d_{ij} = d(\{i\}, \{j\})$.
for $k = n + 1$ **to** $2n - K$ **do**
    Find i and $j > i$ in $\mathcal{I}$ such that d_{ij} is minimal.
    Create a new label set $\mathcal{L}_k := \mathcal{L}_i \cup \mathcal{L}_j$.
    Add the new identifier k to $\mathcal{I}$ and remove the old identifiers i and j from $\mathcal{I}$.
    Update the distance matrix $\mathbf{D}$ with respect to the identifiers i, j, and k.
return $\mathcal{L}_i, i = 1, \dots, 2n - K$

Initially, the distance matrix $\mathbf{D}$ contains the (linkage) distances between the one-point clusters containing one of the data points $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$, and hence with identifiers $1, \dots, n$. Finding the shortest distance amounts to a table lookup in $\mathbf{D}$. When the closest clusters are found, they are merged into a new cluster, and a new identifier k (the smallest positive integer that has not yet been used as an identifier) is assigned to this cluster. The old identifiers i and j are removed from the cluster identifier set $\mathcal{I}$. The matrix $\mathbf{D}$ is then updated by adding a k-th column and row that contain the distances between k and any $m \in \mathcal{I}$. This updating step could be computationally quite costly if the cluster sizes are large and the linkage distance between the clusters depends on all points within the clusters. Fortunately, for many linkage functions, the matrix $\mathbf{D}$ can be updated in an efficient manner.

Suppose that at some stage in the algorithm, clusters $\mathcal{I}$ and $\mathcal{J}$, with identifiers i and j, respectively, are merged into a cluster $\mathcal{K} = \mathcal{I} \cup \mathcal{J}$ with identifier k. Let $\mathcal{M}$, with identifier m, be a previously assigned cluster. An update rule of the linkage distance d_{km} between $\mathcal{K}$ and $\mathcal{M}$ is called a *Lance–Williams* update if it can be written in the form

Lance–Williams

$$d_{km} = \alpha\, d_{im} + \beta\, d_{jm} + \gamma\, d_{ij} + \delta\, |d_{im} - d_{jm}|,$$

where $\alpha, \dots, \delta$ depend only on simple characteristics of the clusters involved, such as the number of elements within the clusters. Table 4.2 shows the update constants for a number of common linkage functions. For example, for single linkage, d_{im} is the minimal distance between $\mathcal{I}$ and $\mathcal{M}$, and d_{jm} is the minimal distance between $\mathcal{J}$ and $\mathcal{M}$. The smallest of these is the minimal distance between $\mathcal{K}$ and $\mathcal{M}$. That is, $d_{km} = \min\{d_{im}, d_{jm}\} = d_{im}/2 + d_{jm}/2 - |d_{im} - d_{jm}|/2$.

Table 4.2: Constants for the Lance–Williams update rule for various linkage functions, with n_i, n_j, n_m denoting the number of elements in the corresponding clusters.

Linkage	α	β	γ	δ
Single	$1/2$	$1/2$	0	$-1/2$
Complete	$1/2$	$1/2$	0	$1/2$
Group avg.	$\frac{n_i}{n_i+n_j}$	$\frac{n_j}{n_i+n_j}$	0	0
Ward	$\frac{n_i+n_m}{n_i+n_j+n_m}$	$\frac{n_j+n_m}{n_i+n_j+n_m}$	$\frac{-n_m}{n_i+n_j+n_m}$	0

LINKAGE MATRIX

In practice, Algorithm 4.7.1 is run until a single cluster is obtained. Instead of returning the label sets of all $2n-1$ clusters, a *linkage matrix* is returned that contains the same information. At the end of each iteration (Line 8) the linkage matrix stores the merged labels i and j, as well as the (minimal) distance d_{ij}. Other information such as the number of elements in the merged cluster can also be stored. Dendrograms and cluster labels can be directly constructed from the linkage matrix. In the following example, the linkage matrix is returned by the method `agg_cluster`.

■ **Example 4.8 (Agglomerative Hierarchical Clustering)** The Python code below gives a basic implementation of Algorithm 4.7.1 using the Ward linkage function. The methods `fcluster` and `dendrogram` from the `scipy` module can be used to identify the labels in a cluster and to draw the corresponding dendrogram.

AggCluster.py

```
import numpy as np
from scipy.spatial.distance import cdist

def update_distances(D,i,j, sizes): # distances for merged cluster
    n = D.shape[0]
    d = np.inf * np.ones(n+1)
    for k in range(n): # Update distances
       d[k] = ((sizes[i]+sizes[k])*D[i,k] +
       (sizes[j]+sizes[k])*D[j,k] -
       sizes[k]*D[i,j])/(sizes[i] + sizes[j] + sizes[k])

    infs =  np.inf * np.ones(n) # array of infinity
    D[i,:],D[:,i],D[j,:],D[:,j] =  infs,infs,infs,infs # deactivate
    new_D = np.inf * np.ones((n+1,n+1))
    new_D[0:n,0:n] = D # copy old matrix into new_D
    new_D[-1,:], new_D[:,-1] = d,d # add new row and column
    return new_D

def agg_cluster(X):
    n = X.shape[0]
    sizes = np.ones(n)
    D = cdist(X, X,metric = 'sqeuclidean') # initialize dist. matrix
        .
    np.fill_diagonal(D, np.inf * np.ones(D.shape[0]))
    Z = np.zeros((n-1,4))  #linkage matrix encodes hierarchy tree
    for t in range(n-1):
```

```
        i,j = np.unravel_index(D.argmin(), D.shape) # minimizer pair
        sizes = np.append(sizes, sizes[i] + sizes[j])
        Z[t,:]=np.array([i, j, np.sqrt(D[i,j]), sizes[-1]])
        D = update_distances(D, i,j, sizes)  # update distance matr.
    return Z

import scipy.cluster.hierarchy as h

X = np.genfromtxt('clusterdata.csv',delimiter=',') # read the data
Z = agg_cluster(X)  # form the linkage matrix

h.dendrogram(Z) # SciPy can produce a dendrogram from Z
# fcluster function assigns cluster ids to all points based on Z
cl = h.fcluster(Z, criterion = 'maxclust', t=3)

import matplotlib.pyplot as plt
plt.figure(2), plt.clf()
cols = ['red','green','blue']
colors = [cols[i-1] for i in cl]
plt.scatter(X[:,0], X[:,1],c=colors)
plt.show()
```

Note that the distance matrix is initialized with the squared Euclidean distance, so that the Ward linkage is rescaled by a factor of 2. Also, note that the linkage matrix stores the square root of the minimal cluster distances rather than the distances themselves. We leave it as an exercise to check that by using these modifications the results agree with the `linkage` method from `scipy`; see Exercise 9. ■

In contrast to the bottom-up (agglomerative) approach to hierarchical clustering, the divisive approach starts with one cluster, which is divided into two clusters that are as "dissimilar" as possible, which can then be further divided, and so on. We can use the same linkage criteria as for agglomerative clustering to divide a parent cluster into two child clusters by *maximizing* the distance between the child clusters. Although it is a natural to try to group together data by separating dissimilar ones as far as possible, the implementation of this idea tends to scale poorly with n. The problem is related to the well-known *max-cut problem*: given an $n \times n$ matrix of positive costs $c_{ij}, i, j \in \{1, \ldots, n\}$, partition the index set $\mathcal{I} = \{1, \ldots, n\}$ into two subsets $\mathcal{J}$ and $\mathcal{K}$ such that the total cost across the sets, that is,

MAX-CUT PROBLEM

$$\sum_{j \in \mathcal{J}} \sum_{k \in \mathcal{K}} d_{jk},$$

is maximal. If instead we maximize according to the *average* distance, we obtain the group average linkage criterion.

■ **Example 4.9 (Divisive Clustering via CE)** The following Python code is used to divide a small data set (of size 300) into two parts according to maximal group average linkage. It uses a short cross-entropy algorithm similar to the one presented in Example 3.19. Given a vector of probabilities $\{p_i, i = 1, \ldots, n\}$, the algorithm generates an $n \times n$ matrix of Bernoulli random variables with success probability p_i for column i. For each row, the 0s and 1s divide the index set into two clusters, and the corresponding average linkage

☞ 110

distance is computed. The matrix is then sorted row-wise according to these distances. Finally, the probabilities $\{p_i\}$ are updated according to the mean values of the best 10% rows. The process is repeated until the $\{p_i\}$ degenerate to a binary vector. This then presents the (approximate) solution.

clustCE2.py

```
import numpy as np
from numpy import genfromtxt
from scipy.spatial.distance import squareform
from scipy.spatial.distance import pdist
import matplotlib.pyplot as plt


def S(x,D):
    V1 = np.where(x==0)[0] # {V1,V2} is the partition
    V2 = np.where(x==1)[0]
    tmp = D[V1]
    tmp = tmp[:,V2]
    return np.mean(tmp) # the size of the cut


def maxcut(D,N,eps,rho,alpha):
    n = D.shape[1]
    Ne = int(rho*N)
    p = 1/2*np.ones(n)
    p[0] = 1.0
    while (np.max(np.minimum(p,np.subtract(1,p))) > eps):
        x = np.array(np.random.uniform(0,1,(N,n))<=p, dtype=np.int64)
        sx = np.zeros(N)
        for i in range(N):
            sx[i] = S(x[i],D)

        sortSX = np.flip(np.argsort(sx))
        #print("gamma = ",sx[sortSX[Ne-1]], " best=",sx[sortSX[0]])
        elIds = sortSX[0:Ne]
        elites = x[elIds]
        pnew = np.mean(elites, axis=0)
        p = alpha*pnew + (1.0-alpha)*p

    return np.round(p)

Xmat = genfromtxt('clusterdata.csv', delimiter=',')
n = Xmat.shape[0]
D = squareform(pdist(Xmat))
N = 1000
eps = 10**-2
rho = 0.1
alpha = 0.9

# CE
pout = maxcut(D,N,eps,rho, alpha);

cutval = S(pout,D)
```

```
print("cutvalue ",cutval)

#plot
V1 = np.where(pout==0)[0]
xblue = Xmat[V1]
V2 = np.where(pout==1)[0]
xred = Xmat[V2]
plt.scatter(xblue[:,0],xblue[:,1], c="blue")
plt.scatter(xred[:,0],xred[:,1], c="red")
```

```
cutvalue  4.625207676517948
```

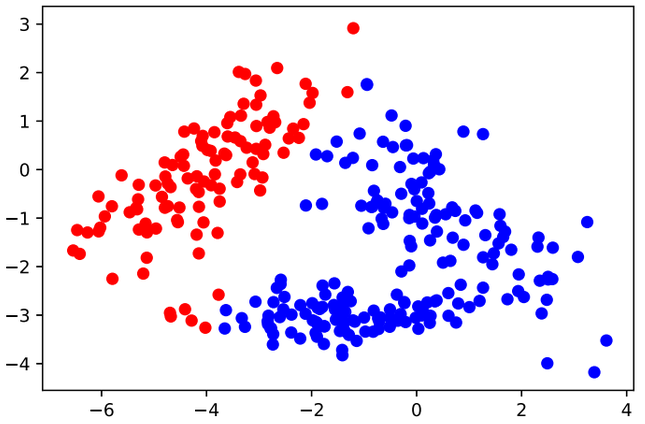


Figure 4.11: Division of the data in Figure 4.4 into two clusters, via the cross-entropy method.

4.8 Principal Component Analysis (PCA)

PRINCIPAL COMPONENT ANALYSIS

The main idea of *principal component analysis* (PCA) is to reduce the dimensionality of a data set consisting of many variables. PCA is a *feature reduction* (or *feature extraction*) mechanism, that helps us to handle high-dimensional data with more features than is convenient to interpret.

4.8.1 Motivation: Principal Axes of an Ellipsoid

Consider a d-dimensional normal distribution with mean vector $\mathbf{0}$ and covariance matrix $\boldsymbol{\Sigma}$. The corresponding pdf (see (2.33)) is ☞ 45

$$f(\boldsymbol{x}) = \frac{1}{\sqrt{(2\pi)^n \, |\boldsymbol{\Sigma}|}} \, \mathrm{e}^{-\frac{1}{2} \boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1} \boldsymbol{x}}, \quad \boldsymbol{x} \in \mathbb{R}^d.$$

If we were to draw many iid samples from this pdf, the points would roughly have an *ellipsoid* pattern, as illustrated in Figure 3.1, and correspond to the contours of f: sets of ☞ 71

points $\boldsymbol{x}$ such that $\boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1} \boldsymbol{x} = c$, for some $c \geqslant 0$. In particular, consider the ellipsoid

$$\boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1} \boldsymbol{x} = 1, \quad \boldsymbol{x} \in \mathbb{R}^d. \tag{4.42}$$

☞ 375
☞ 368

PRINCIPAL AXES

SINGULAR VALUE DECOMPOSITION

☞ 380

Let $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$, where $\mathbf{B}$ is for example the (lower) Cholesky matrix. Then, as explained in Example A.5, the ellipsoid (4.42) can also be viewed as the linear transformation of d-dimensional unit sphere via matrix $\mathbf{B}$. Moreover, the *principal axes* of the ellipsoid can be found via a *singular value decomposition* (SVD) of $\mathbf{B}$ (or $\boldsymbol{\Sigma}$); see Section A.6.5 and Example A.8. In particular, suppose that an SVD of $\mathbf{B}$ is

$$\mathbf{B} = \mathbf{U}\mathbf{D}\mathbf{V}^\top \qquad \text{(note that an SVD of } \boldsymbol{\Sigma} \text{ is then } \mathbf{U}\mathbf{D}^2\mathbf{U}^\top\text{)}.$$

The columns of the matrix $\mathbf{UD}$ correspond to the principal axes of the ellipsoid, and the relative magnitudes of the axes are given by the elements of the diagonal matrix $\mathbf{D}$. If some of these magnitudes are small compared to the others, a reduction in the dimension of the space may be achieved by *projecting* each point $\boldsymbol{x} \in \mathbb{R}^d$ onto the subspace spanned by the main (say $k \ll d$) columns of $\mathbf{U}$ — the so-called *principal components*. Suppose without loss of generality that the first k principal components are given by the first k columns of $\mathbf{U}$, and let $\mathbf{U}_k$ be the corresponding $d \times k$ matrix.

PRINCIPAL COMPONENTS

With respect to the standard basis $\{\boldsymbol{e}_i\}$, the vector $\boldsymbol{x} = x_1\boldsymbol{e}_1 + \cdots + x_d\boldsymbol{e}_d$ is represented by the d-dimensional vector $[x_1, \ldots, x_d]^\top$. With respect to the orthonormal basis $\{\boldsymbol{u}_i\}$ formed by the columns of matrix $\mathbf{U}$, the representation of $\boldsymbol{x}$ is $\mathbf{U}^\top\boldsymbol{x}$. Similarly, the projection of any point $\boldsymbol{x}$ onto the subspace spanned by the first k principal vectors is represented by the k-dimensional vector $\mathbf{U}_k^\top\boldsymbol{x}$, with respect to the orthonormal basis formed by the columns of $\mathbf{U}_k$. So, the idea is that if a point $\boldsymbol{x}$ lies close to its projection $\mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}$, we may represent it via k numbers instead of d, using the combined features given by the k principal components. See Section A.4 for a review of projections and orthonormal bases.

☞ 364

■ **Example 4.10 (Principal Components)** Consider the matrix

$$\boldsymbol{\Sigma} = \begin{bmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{bmatrix},$$

which can be written as $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$, with

$$\mathbf{B} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}.$$

Figure 4.12 depicts the ellipsoid $\boldsymbol{x}^\top\boldsymbol{\Sigma}^{-1}\boldsymbol{x} = 1$, which can be obtained by linearly transforming the points on the unit sphere by means of the matrix $\mathbf{B}$. The principal axes and sizes of the ellipsoid are found through a singular value decomposition $\mathbf{B} = \mathbf{U}\mathbf{D}\mathbf{V}^\top$, where $\mathbf{U}$ and $\mathbf{D}$ are

$$\mathbf{U} = \begin{bmatrix} 0.8460 & 0.4828 & 0.2261 \\ 0.4973 & -0.5618 & -0.6611 \\ 0.1922 & -0.6718 & 0.7154 \end{bmatrix} \quad \text{and} \quad \mathbf{D} = \begin{bmatrix} 4.4027 & 0 & 0 \\ 0 & 0.7187 & 0 \\ 0 & 0 & 0.3160 \end{bmatrix}.$$

The columns of $\mathbf{U}$ show the directions of the principal axes of the ellipsoid, and the diagonal elements of $\mathbf{D}$ indicate the relative magnitudes of the principal axes. We see that the first principal component is given by the first column of $\mathbf{U}$, and the second principal component by the second column of $\mathbf{U}$.

The projection of the point $\boldsymbol{x} = [1.052, 0.6648, 0.2271]^\top$ onto the 1-dimensional space spanned by the first principal component $\boldsymbol{u}_1 = [0.8460, 0.4972, 0.1922]^\top$ is $\boldsymbol{z} = \boldsymbol{u}_1\boldsymbol{u}_1^\top\boldsymbol{x} = [1.0696, 0.6287, 0.2429]^\top$. With respect to the basis vector $\boldsymbol{u}_1$, $\boldsymbol{z}$ is represented by the number $\boldsymbol{u}_1^\top\boldsymbol{z} = 1.2643$. That is, $\boldsymbol{z} = 1.2643\boldsymbol{u}_1$.

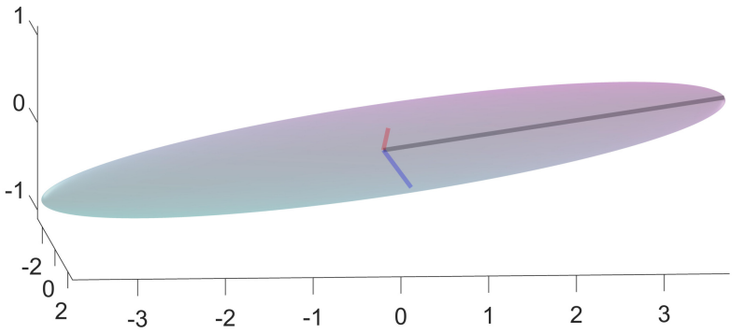


Figure 4.12: A "surfboard" ellipsoid where one principal axis is significantly larger than the other two.

■

4.8.2 PCA and Singular Value Decomposition (SVD)

In the setting above, we did not consider any data set drawn from a multivariate pdf f. The whole analysis rested on linear algebra. In *principal component analysis* (PCA) we start with data $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, where each $\boldsymbol{x}$ is d-dimensional. PCA does not require assumptions how the data were obtained, but to make the link with the previous section, we can think of the data as iid draws from a multivariate normal pdf.

PRINCIPAL COMPONENT ANALYSIS

Let us collect the data in a matrix $\mathbf{X}$ in the usual way; that is,

☞ 43

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} & \ldots & x_{1d} \\ x_{21} & x_{22} & \ldots & x_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \ldots & x_{nd} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}_1^\top \\ \boldsymbol{x}_2^\top \\ \vdots \\ \boldsymbol{x}_n^\top \end{bmatrix}.$$

The matrix $\mathbf{X}$ will be the PCA's input. Under this setting, the data consists of points in d-dimensional space, and our goal is to present the data using n feature vectors of dimension $k < d$.

In accordance with the previous section, we assume that underlying distribution of the data has expectation vector $\mathbf{0}$. In practice, this means that before PCA is applied, the data needs to be *centered* by subtracting the *column* mean in every column:

$$x'_{ij} = x_{ij} - \overline{x}_j,$$

where $\overline{x}_j = \frac{1}{n}\sum_{i=1}^n x_{ij}$.

We assume from now on that the data comes from a general d-dimensional distribution with mean vector $\mathbf{0}$ and some covariance matrix $\boldsymbol{\Sigma}$. The covariance matrix $\boldsymbol{\Sigma}$ is by definition equal to the expectation of the random matrix $\boldsymbol{X}\boldsymbol{X}^\top$, and can be estimated from the data $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ via the sample average

$$\widehat{\boldsymbol{\Sigma}} = \frac{1}{n}\sum_{i=1}^n \boldsymbol{x}_i \boldsymbol{x}_i^\top = \frac{1}{n}\mathbf{X}^\top\mathbf{X}.$$

As $\widehat{\boldsymbol{\Sigma}}$ is a covariance matrix, we may conduct the same analysis for $\widehat{\boldsymbol{\Sigma}}$ as we did for $\boldsymbol{\Sigma}$ in the previous section. Specifically, suppose $\widehat{\boldsymbol{\Sigma}} = \mathbf{U}\mathbf{D}^2\mathbf{U}^\top$ is an SVD of $\widehat{\boldsymbol{\Sigma}}$ and let $\mathbf{U}_k$ be the matrix whose columns are the k principal components; that is, the k columns of $\mathbf{U}$ corresponding to the largest diagonal elements in $\mathbf{D}^2$. Note that we have used $\mathbf{D}^2$ instead of $\mathbf{D}$ to be compatible with the previous section. The transformation $\boldsymbol{z}_i = \mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i$ maps each vector $\boldsymbol{x}_i \in \mathbb{R}^d$ (thus, with d features) to a vector $\boldsymbol{z}_i \in \mathbb{R}^d$ lying in the subspace spanned by the columns of $\mathbf{U}_k$. With respect to this basis, the point $\boldsymbol{z}_i$ has representation $\boldsymbol{z}_i = \mathbf{U}_k^\top(\mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i) = \mathbf{U}_k^\top\boldsymbol{x}_i \in \mathbb{R}^k$ (thus with k features). The corresponding covariance matrix of the $\boldsymbol{z}_i, i = 1, \ldots, n$ is diagonal. The diagonal elements $\{d_{\ell\ell}\}$ of $\mathbf{D}$ can be interpreted as standard deviations of the data in the directions of the principal components. The quantity $v = \sum_{\ell=1} d_{\ell\ell}^2$ (that is, the trace of $\mathbf{D}^2$) is thus a measure for the amount of variance in the data. The proportion $d_{\ell\ell}^2/v$ indicates how much of the variance in the data is explained by the ℓ-th principal component.

Another way to look at PCA is by considering the question: How can we best project the data onto a k-dimensional subspace in such a way that the total squared distance between
☞ 364
the projected points and the original points is minimal? From Section A.4, we know that any orthogonal projection to a k-dimensional subspace $\mathcal{V}_k$ can be represented by a matrix $\mathbf{U}_k\mathbf{U}_k^\top$, where $\mathbf{U}_k = [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k]$ and the $\{\boldsymbol{u}_\ell, \ell = 1, \ldots, k\}$ are orthogonal vectors of length 1 that span $\mathcal{V}_k$. The above question can thus be formulated as the minimization program:

$$\min_{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_k} \sum_{i=1}^n \|\boldsymbol{x}_i - \mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i\|^2. \tag{4.43}$$

Now observe that

$$\begin{aligned}
\frac{1}{n}\sum_{i=1}^n \|\boldsymbol{x}_i - \mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i\|^2 &= \frac{1}{n}\sum_{i=1}^n (\boldsymbol{x}_i^\top - \boldsymbol{x}_i^\top\mathbf{U}_k\mathbf{U}_k^\top)(\boldsymbol{x}_i - \mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i) \\
&= \underbrace{\frac{1}{n}\sum_{i=1}^n \|\boldsymbol{x}_i\|^2}_{c} - \frac{1}{n}\sum_{i=1}^n \boldsymbol{x}_i^\top\mathbf{U}_k\mathbf{U}_k^\top\boldsymbol{x}_i = c - \frac{1}{n}\sum_{i=1}^n\sum_{\ell=1}^k \operatorname{tr}(\boldsymbol{x}_i^\top\boldsymbol{u}_\ell\boldsymbol{u}_\ell^\top\boldsymbol{x}_i) \\
&= c - \frac{1}{n}\sum_{\ell=1}^k\sum_{i=1}^n \boldsymbol{u}_\ell^\top\boldsymbol{x}_i\boldsymbol{x}_i^\top\boldsymbol{u}_\ell = c - \sum_{\ell=1}^k \boldsymbol{u}_\ell^\top\widehat{\boldsymbol{\Sigma}}\boldsymbol{u}_\ell,
\end{aligned}$$

☞ 359
where we have used the cyclic property of a trace (Theorem A.1) and the fact that $\mathbf{U}_k\mathbf{U}_k^\top$ can be written as $\sum_{\ell=1}^k \boldsymbol{u}_\ell\boldsymbol{u}_\ell^\top$. It follows that the minimization problem(4.43) is equivalent to the maximization problem

$$\max_{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_k} \sum_{\ell=1}^k \boldsymbol{u}_\ell^\top\widehat{\boldsymbol{\Sigma}}\boldsymbol{u}_\ell. \tag{4.44}$$

This maximum can be at most $\sum_{\ell=1}^{k} d_{\ell\ell}^2$ and is attained precisely when $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ are the first k principal components of $\widehat{\boldsymbol{\Sigma}}$.

■ **Example 4.11 (Singular Value Decomposition)** The following data set consists of independent samples from the three-dimensional Gaussian distribution with mean vector $\mathbf{0}$ and covariance matrix $\boldsymbol{\Sigma}$ given in Example 4.10:

$$\mathbf{X} = \begin{bmatrix} 3.1209 & 1.7438 & 0.5479 \\ -2.6628 & -1.5310 & -0.2763 \\ 3.7284 & 3.0648 & 1.8451 \\ 0.4203 & 0.3553 & 0.4268 \\ -0.7155 & -0.6871 & -0.1414 \\ 5.8728 & 4.0180 & 1.4541 \\ 4.8163 & 2.4799 & 0.5637 \\ 2.6948 & 1.2384 & 0.1533 \\ -1.1376 & -0.4677 & -0.2219 \\ -1.2452 & -0.9942 & -0.4449 \end{bmatrix}.$$

After replacing $\mathbf{X}$ with its centered version, an SVD $\mathbf{U}\mathbf{D}^2\mathbf{U}^\top$ of $\widehat{\boldsymbol{\Sigma}} = \mathbf{X}^\top\mathbf{X}/n$ yields the principal component matrix $\mathbf{U}$ and diagonal matrix $\mathbf{D}$:

$$\mathbf{U} = \begin{bmatrix} -0.8277 & 0.4613 & 0.3195 \\ -0.5300 & -0.4556 & -0.7152 \\ -0.1843 & -0.7613 & 0.6216 \end{bmatrix} \quad \text{and} \quad \mathbf{D} = \begin{bmatrix} 3.3424 & 0 & 0 \\ 0 & 0.4778 & 0 \\ 0 & 0 & 0.1038 \end{bmatrix}.$$

We also observe that, apart from the sign of the first column, the principal component matrix $\mathbf{U}$ is similar to that in Example 4.10. Likewise for the matrix $\mathbf{D}$. We see that 97.90% of the total variance is explained by the first principal component. Figure 4.13 shows the projection of the centered data onto the subspace spanned by this principal component.

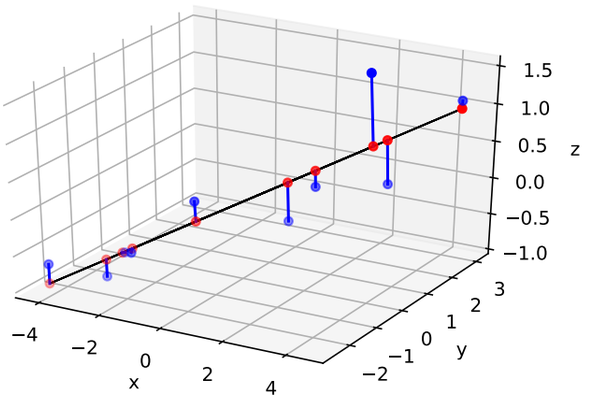


Figure 4.13: Data from the "surfboard" pdf is projected onto the subspace spanned by the largest principal component.

The following Python code was used.

PCAdat.py

```
import numpy as np
X = np.genfromtxt('pcadat.csv', delimiter=',')
n = X.shape[0]

X = X - X.mean(axis=0)
G = X.T @ X
U, _ , _ = np.linalg.svd(G/n)

# projected points
Y = X @ np.outer(U[:,0],U[:,0])

import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D

fig = plt.figure()
ax = fig.add_subplot(111, projection='3d')
ax.w_xaxis.set_pane_color((0, 0, 0, 0))
ax.plot(Y[:,0], Y[:,1], Y[:,2], c='k', linewidth=1)
ax.scatter(X[:,0], X[:,1], X[:,2], c='b')
ax.scatter(Y[:,0], Y[:,1], Y[:,2], c='r')

for i in range(n):
    ax.plot([X[i,0], Y[i,0]], [X[i,1],Y[i,1]], [X[i,2],Y[i,2]], 'b')

ax.set_xlabel('x')
ax.set_ylabel('y')
ax.set_zlabel('z')
plt.show()
```

■

Next is an application of PCA to Fisher's famous **iris** data set, already mentioned in ☞ 2 Section 1.1, and Exercise 1.5.

■ **Example 4.12 (PCA for the Iris Data Set)** The **iris** data set contains measurements on four features of the iris plant: sepal length and width, and petal length and width, for a total of 150 specimens. The full data set also contains the species name, but for the purpose of this example we ignore it.

☞ 17 Figure 1.9 shows that there is a significant correlation between the different features. Can we perhaps describe the data using fewer features by taking certain linear combinations of the original features? To investigate this, let us perform a PCA, first centering the data. The following Python code implements the PCA. It is assumed that a CSV file `irisX.csv` has been made that contains the iris data set (without the species information).

PCAiris.py

```
import seaborn as sns, numpy as np
np.set_printoptions(precision=4)

X = np.genfromtxt('IrisX.csv',delimiter=',')
n = X.shape[0]
```

```
X = X - np.mean(X, axis=0)

[U,D2,UT]= np.linalg.svd((X.T @ X)/n)
print('U = \n', U); print('\n diag(D^2) = ', D2)

z =  U[:,0].T @ X.T

sns.kdeplot(z, bw=0.15)
```

```
U =
 [[-0.3614 -0.6566  0.582   0.3155]
 [ 0.0845 -0.7302 -0.5979 -0.3197]
 [-0.8567  0.1734 -0.0762 -0.4798]
 [-0.3583  0.0755 -0.5458  0.7537]]

 diag(D^2) =  [4.2001 0.2411 0.0777 0.0237]
```

The output above shows the principal component matrix (which we called $\mathbf{U}$) as well as the diagonal of matrix $\mathbf{D}^2$. We see that a large proportion of the variance, $4.2001/(4.2001 + 0.2411 + 0.0777 + 0.0237) = 92.46\%$, is explained by the first principal component. Thus, it makes sense to transform each data point $\boldsymbol{x} \in \mathbb{R}^4$ to $\boldsymbol{u}_1^\top \boldsymbol{x} \in \mathbb{R}$. Figure 4.14 shows the kernel density estimate of the transformed data. Interestingly, we see two modes, indicating at least two clusters in the data.

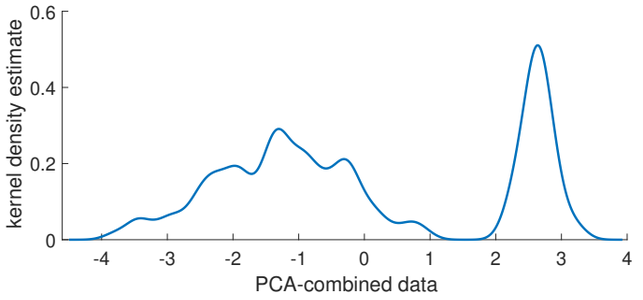


Figure 4.14: Kernel density estimate of the PCA-combined `iris` data.

Further Reading

Various information-theoretic measures to quantify uncertainty, including the Shannon entropy and Kullback–Leibler divergence, may be found in [28]. The Fisher information, the prominent information measure in statistics, is discussed in detail in [78]. Akaike's information criterion appeared in [2]. The EM algorithm was introduced in [31] and [85] gives an in-depth treatment. Convergence proofs for the EM algorithm may be found in [19, 128]. A classical reference on kernel density estimation is [113], and [14] is the main reference for the theta kernel density estimator. Theory and applications on finite mixture models may be found in [86]. For more details on clustering applications and algorithms as well as references on data compression, vector quantization, and pattern recognition, we refer

to [1, 35, 107, 125]. A useful modification of the K-means algorithm is the *fuzzy K-means* algorithm; see, e.g., [9]. A popular way to choose the starting positions in K-means is given by the K-means++ heuristic, introduced in [4].

Exercises

1. This exercise is to show that the Fisher information matrix $\mathbf{F}(\boldsymbol{\theta})$ in (4.8) is equal to the matrix $\mathbf{H}(\boldsymbol{\theta})$ in (4.9), in the special case where $f = g(\cdot \,|\, \boldsymbol{\theta})$, and under the assumption that integration and differentiation orders can be interchanged.

QUOTIENT RULE FOR DIFFERENTIATION

(a) Let $\boldsymbol{h}$ be a vector-valued function and k a real-valued function. Prove the following *quotient rule for differentiation*:

$$\frac{\partial[\boldsymbol{h}(\boldsymbol{\theta})/k(\boldsymbol{\theta})]}{\partial \boldsymbol{\theta}} = \frac{1}{k(\boldsymbol{\theta})}\frac{\partial \boldsymbol{h}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} - \frac{1}{k^2(\boldsymbol{\theta})}\frac{\partial k(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}}\boldsymbol{h}(\boldsymbol{\theta})^\top. \tag{4.45}$$

(b) Now take $\boldsymbol{h}(\boldsymbol{\theta}) = \frac{\partial g(\boldsymbol{X}\,|\,\boldsymbol{\theta})}{\partial \boldsymbol{\theta}}$ and $k(\boldsymbol{\theta}) = g(\boldsymbol{X}\,|\,\boldsymbol{\theta})$ in (4.45) and take expectations with respect to $\mathbb{E}_{\boldsymbol{\theta}}$ on both sides to show that

$$-\mathbf{H}(\boldsymbol{\theta}) = \underbrace{\mathbb{E}_{\boldsymbol{\theta}}\left[\frac{1}{g(\boldsymbol{X}\,|\,\boldsymbol{\theta})}\frac{\partial \frac{\partial g(\boldsymbol{X}\,|\,\boldsymbol{\theta})}{\partial \boldsymbol{\theta}}}{\partial \boldsymbol{\theta}}\right]}_{\mathbf{A}} - \mathbf{F}(\boldsymbol{\theta}).$$

(c) Finally show that $\mathbf{A}$ is the zero matrix.

2. Plot the mixture of $\mathcal{N}(0,1)$, $\mathcal{U}(0,1)$, and $\mathsf{Exp}(1)$ distributions, with weights $w_1 = w_2 = w_3 = 1/3$.

3. Denote the pdfs in Exercise 2 by f_1, f_2, f_3, respectively. Suppose that X is simulated via the two-step procedure: First, draw Z from $\{1,2,3\}$, then draw X from f_Z. How likely is it that the outcome $x = 0.5$ of X has come from the uniform pdf f_2?

4. Simulate an iid training set of size 100 from the $\mathsf{Gamma}(2.3, 0.5)$ distribution, and implement the Fisher scoring method in Example 4.1 to find the maximum likelihood estimate. Plot the true and approximate pdfs.

5. Let $\mathcal{T} = \{\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n\}$ be iid data from a pdf $g(\boldsymbol{x}\,|\,\boldsymbol{\theta})$ with Fisher matrix $\mathbf{F}(\boldsymbol{\theta})$. Explain why, under the conditions where (4.7) holds,

$$\boldsymbol{S}_{\mathcal{T}}(\boldsymbol{\theta}) := \frac{1}{n}\sum_{i=1}^{n} \boldsymbol{S}(\boldsymbol{X}_i\,|\,\boldsymbol{\theta})$$

for large n has approximately a multivariate normal distribution with expectation vector $\mathbf{0}$ and covariance matrix $\mathbf{F}(\boldsymbol{\theta})/n$.

6. Figure 4.15 shows a Gaussian KDE with bandwidth $\sigma = 0.2$ on the points $-0.5, 0, 0.2, 0.9$, and 1.5. Reproduce the plot in Python. Using the same bandwidth, plot also the KDE for the same data, but now with $\phi(z) = 1/2, z \in [-1, 1]$.

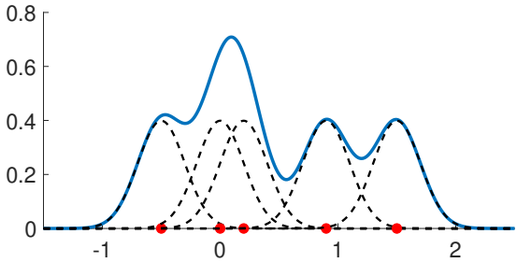


Figure 4.15: The Gaussian KDE (solid line) is the equally weighted mixture of normal pdfs centered around the data and with standard deviation $\sigma = 0.2$ (dashed).

7. For fixed x', the Gaussian kernel function

$$f(x\,|\,t) := \frac{1}{\sqrt{2\pi t}}\,\mathrm{e}^{-\frac{1}{2}\frac{(x-x')^2}{t}}$$

is the solution to Fourier's *heat equation*

$$\frac{\partial}{\partial t} f(x\,|\,t) = \frac{1}{2}\frac{\partial^2}{\partial x^2} f(x\,|\,t), \quad x \in \mathbb{R},\ t > 0,$$

with initial condition $f(x\,|\,0) = \delta(x - x')$ (the Dirac function at x'). Show this. As a consequence, the Gaussian KDE is the solution to the same heat equation, but now with initial condition $f(x\,|\,0) = n^{-1}\sum_{i=1}^{n}\delta(x - x_i)$. This was the motivation for the theta KDE [14], which is a solution to the same heat equation but now on a *bounded* interval.

8. Show that the Ward linkage given in (4.41) is equal to

$$d_{\text{Ward}}(\mathcal{I}, \mathcal{J}) = \frac{|\mathcal{I}|\,|\mathcal{J}|}{|\mathcal{I}| + |\mathcal{J}|}\|\overline{\boldsymbol{x}}_{\mathcal{I}} - \overline{\boldsymbol{x}}_{\mathcal{J}}\|^2.$$

9. Carry out the agglomerative hierarchical clustering of Example 4.8 via the `linkage` method from `scipy.cluster.hierarchy`. Show that the linkage matrices are the same. Give a scatterplot of the data, color coded into $K = 3$ clusters.

10. Suppose that we have the data $\tau_n = \{x_1, \ldots, x_n\}$ in $\mathbb{R}$ and decide to train the two-component Gaussian mixture model

$$g(x\,|\,\boldsymbol{\theta}) = w_1 \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_1^2}\right) + w_2 \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{(x-\mu_2)^2}{2\sigma_2^2}\right),$$

where the parameter vector $\boldsymbol{\theta} = [\mu_1, \mu_2, \sigma_1, \sigma_2, w_1, w_2]^\top$ belongs to the set

$$\Theta = \{\boldsymbol{\theta} : w_1 + w_2 = 1, w_1 \in [0,1], \mu_i \in \mathbb{R}, \sigma_i > 0,\ \forall i\}.$$

Suppose that the training is via the maximum likelihood in (2.28). Show that

$$\sup_{\boldsymbol{\theta}\in\Theta} \frac{1}{n}\sum_{i=1}^{n} \ln g(x_i\,|\,\boldsymbol{\theta}) = \infty.$$

In other words, find a sequence of values for $\boldsymbol{\theta} \in \Theta$ such that the likelihood grows without bound. How can we restrict the set Θ to ensure that the likelihood remains bounded?

11. A d-dimensional normal random vector $\boldsymbol{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ can be defined via an affine transformation, $\boldsymbol{X} = \boldsymbol{\mu} + \boldsymbol{\Sigma}^{1/2}\boldsymbol{Z}$, of a standard normal random vector $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_d)$, where $\boldsymbol{\Sigma}^{1/2}(\boldsymbol{\Sigma}^{1/2})^\top = \Sigma$. In a similar way, we can define a d-dimensional Student random vector $\boldsymbol{X} \sim \mathrm{t}_\alpha(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ via a transformation

$$\boldsymbol{X} = \boldsymbol{\mu} + \frac{1}{\sqrt{S}}\boldsymbol{\Sigma}^{1/2}\boldsymbol{Z}, \tag{4.46}$$

where, $\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_d)$ and $S \sim \mathsf{Gamma}(\frac{\alpha}{2}, \frac{\alpha}{2})$ are independent, $\alpha > 0$, and $\boldsymbol{\Sigma}^{1/2}(\boldsymbol{\Sigma}^{1/2})^\top = \Sigma$. Note that we obtain the multivariate normal distribution as a limiting case for $\alpha \to \infty$.

(a) Show that the density of the $\mathrm{t}_\alpha(\mathbf{0}, \mathbf{I}_d)$ distribution is given by

$$t_\alpha(\boldsymbol{x}) := \frac{\Gamma((\alpha+d)/2)}{(\pi\alpha)^{d/2}\Gamma(\alpha/2)}\left(1 + \frac{1}{\alpha}\|\boldsymbol{x}\|^2\right)^{-\frac{\alpha+d}{2}}.$$

☞ 435 By the transformation rule (C.23), it follows that the density of $\boldsymbol{X} \sim \mathrm{t}_\alpha(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ is given by $t_{\alpha,\boldsymbol{\Sigma}}(\boldsymbol{x} - \boldsymbol{\mu})$, where

$$t_{\alpha,\boldsymbol{\Sigma}}(\boldsymbol{x}) := \frac{1}{|\boldsymbol{\Sigma}^{1/2}|}t_\alpha(\boldsymbol{\Sigma}^{-1/2}\boldsymbol{x}).$$

[Hint: conditional on $S = s$, $\boldsymbol{X}$ has a $\mathcal{N}(\mathbf{0}, \mathbf{I}_d/s)$ distribution.]

(b) We wish to fit a $\mathbf{t}_\nu(\boldsymbol{\mu}, \Sigma)$ distribution to given data $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ in $\mathbb{R}^d$ via the EM method. We use the representation (4.46) and augment the data with the vector $\boldsymbol{S} = [S_1, \ldots, S_n]^\top$ of hidden variables. Show that the complete-data likelihood is given by

$$g(\tau, \boldsymbol{s} \,|\, \boldsymbol{\theta}) = \prod_i \frac{(\alpha/2)^{\alpha/2} s_i^{(\alpha+d)/2-1} \exp(-\frac{s_i}{2}\alpha - \frac{s_i}{2}\|\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu})\|^2)}{\Gamma(\alpha/2)(2\pi)^{d/2}|\boldsymbol{\Sigma}^{1/2}|}. \tag{4.47}$$

(c) Show that, as a consequence, conditional on the data τ and parameter $\boldsymbol{\theta}$, the hidden data are mutually independent, and

$$(S_i \,|\, \tau, \boldsymbol{\theta}) \sim \mathsf{Gamma}\left(\frac{\alpha+d}{2}, \frac{\alpha + \|\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu})\|^2}{2}\right), \quad i = 1, \ldots, n.$$

(d) At iteration t of the EM algorithm, let $g^{(t)}(\boldsymbol{s}) = g(\boldsymbol{s} \,|\, \tau, \boldsymbol{\theta}^{(t-1)})$ be the density of the missing data, given the observed data τ and the current parameter guess $\boldsymbol{\theta}^{(t-1)}$. Verify that the expected complete-data log-likelihood is given by:

$$\begin{aligned}\mathbb{E}_{g^{(t)}} \ln g(\tau, \boldsymbol{S} \,|\, \boldsymbol{\theta}) = {} & \frac{n\alpha}{2}\ln\frac{\alpha}{2} - \frac{nd}{2}\ln(2\pi) - n\ln\Gamma\left(\frac{\alpha}{2}\right) - \frac{n}{2}\ln|\boldsymbol{\Sigma}| \\ & + \frac{\alpha+d-2}{2}\sum_{i=1}^n \mathbb{E}_{g^{(t)}} \ln S_i - \sum_{i=1}^n \frac{\alpha + \|\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu})\|^2}{2}\mathbb{E}_{g^{(t)}} S_i.\end{aligned}$$

Show that

$$\begin{aligned}\mathbb{E}_{g^{(t)}} S_i &= \frac{\alpha^{(t-1)} + d}{\alpha^{(t-1)} + \|(\boldsymbol{\Sigma}^{(t-1)})^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu}^{(t-1)})\|^2} =: w_i^{(t-1)} \\ \mathbb{E}_{g^{(t)}} \ln S_i &= \psi\left(\frac{\alpha^{(t-1)}+d}{2}\right) - \ln\left(\frac{\alpha^{(t-1)}+d}{2}\right) + \ln w_i^{(t-1)},\end{aligned}$$

where $\psi := (\ln\Gamma)'$ is *digamma* function.

(e) Finally, show that in the M-step of the EM algorithm $\boldsymbol{\theta}^{(t)}$ is updated from $\boldsymbol{\theta}^{(t-1)}$ as follows:

$$\boldsymbol{\mu}^{(t)} = \frac{\sum_{i=1}^n w_i^{(t-1)} \boldsymbol{x}_i}{\sum_{i=1}^n w_i^{(t-1)}}$$
$$\boldsymbol{\Sigma}^{(t)} = \frac{1}{n} \sum_{i=1}^n w_i^{(t-1)} (\boldsymbol{x}_i - \boldsymbol{\mu}^{(t)})(\boldsymbol{x}_i - \boldsymbol{\mu}^{(t)})^\top,$$

and $\alpha^{(t)}$ is defined implicitly through the solution of the nonlinear equation:

$$\ln\left(\frac{\alpha}{2}\right) - \psi\left(\frac{\alpha}{2}\right) + \psi\left(\frac{\alpha^{(t)} + d}{2}\right) - \ln\left(\frac{\alpha^{(t)} + d}{2}\right) + 1 + \frac{\sum_{i=1}^n \left(\ln(w_i^{(t-1)}) - w_i^{(t-1)}\right)}{n} = 0.$$

12. A generalization of both the gamma and inverse-gamma distribution is the *generalized inverse-gamma distribution*, which has density

GENERALIZED INVERSE-GAMMA DISTRIBUTION

$$f(s) = \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} s^{p-1} \mathrm{e}^{-\frac{1}{2}(as+b/s)}, \quad a, b, s > 0, \ p \in \mathbb{R}, \tag{4.48}$$

where K_p is the *modified Bessel function of the second kind*, which can be defined as the integral

MODIFIED BESSEL FUNCTION OF THE SECOND KIND

$$K_p(x) = \int_0^\infty \mathrm{e}^{-x\cosh(t)} \cosh(pt)\, \mathrm{d}t, \quad x > 0, \ p \in \mathbb{R}. \tag{4.49}$$

We write $S \sim \mathsf{GIG}(a, b, p)$ to denote that S has a pdf of the form (4.48). The function K_p has many interesting properties. Special cases include

$$K_{1/2}(x) = \sqrt{\frac{x\pi}{2}}\, \mathrm{e}^{-x}\, \frac{1}{x}$$
$$K_{3/2}(x) = \sqrt{\frac{x\pi}{2}}\, \mathrm{e}^{-x} \left(\frac{1}{x} + \frac{1}{x^2}\right)$$
$$K_{5/2}(x) = \sqrt{\frac{x\pi}{2}}\, \mathrm{e}^{-x} \left(\frac{1}{x} + \frac{3}{x^2} + \frac{3}{x^3}\right).$$

More generally, K_p satisfies the recursion

$$K_{p+1}(x) = K_{p-1}(x) + \frac{2p}{x} K_p(x). \tag{4.50}$$

(a) Using the change of variables $\mathrm{e}^z = s\sqrt{a/b}$, show that

$$\int_0^\infty s^{p-1} \mathrm{e}^{-\frac{1}{2}(as+b/s)}\, \mathrm{d}s = 2K_p(\sqrt{ab})(b/a)^{p/2}.$$

(b) Let $S \sim \mathsf{GIG}(a, b, p)$. Show that

$$\mathbb{E}S = \frac{\sqrt{b}\, K_{p+1}(\sqrt{ab})}{\sqrt{a}\, K_p(\sqrt{ab})} \tag{4.51}$$

and

$$\mathbb{E}S^{-1} = \frac{\sqrt{a}\, K_{p+1}(\sqrt{ab})}{\sqrt{b}\, K_p(\sqrt{ab})} - \frac{2p}{b}. \tag{4.52}$$

SCALE-MIXTURE

13. In Exercise 11 we viewed the multivariate Student t_α distribution as a *scale-mixture* of the $\mathcal{N}(\mathbf{0}, \mathbf{I}_d)$ distribution. In this exercise, we consider a similar transformation, but now $\boldsymbol{\Sigma}^{1/2}\boldsymbol{Z} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma})$ is not divided but is *multiplied* by $\sqrt{S}$, with $S \sim \mathsf{Gamma}(\alpha/2, \alpha/2)$:

$$\boldsymbol{X} = \boldsymbol{\mu} + \sqrt{S}\,\boldsymbol{\Sigma}^{1/2}\,\boldsymbol{Z}, \tag{4.53}$$

where S and $\boldsymbol{Z}$ are independent and $\alpha > 0$.

BESSEL DISTRIBUTION

(a) Show, using Exercise 12, that for $\boldsymbol{\Sigma}^{1/2} = \mathbf{I}_d$ and $\boldsymbol{\mu} = \mathbf{0}$, the random vector $\boldsymbol{X}$ has a d-dimensional *Bessel distribution*, with density:

$$\kappa_\alpha(\boldsymbol{x}) := \frac{2^{1-(\alpha+d)/2}\alpha^{(\alpha+d)/4}\,\|\boldsymbol{x}\|^{(\alpha-d)/2}}{\pi^{d/2}\Gamma(\alpha/2)} K_{(\alpha-d)/2}\left(\|\boldsymbol{x}\|\sqrt{\alpha}\right), \quad \boldsymbol{x} \in \mathbb{R}^d,$$

where K_p is the modified Bessel function of the second kind given in (4.49). We write $\boldsymbol{X} \sim \mathsf{Bessel}_\alpha(\mathbf{0}, \mathbf{I}_d)$. A random vector $\boldsymbol{X}$ is said to have a $\mathsf{Bessel}_\alpha(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ distribution if it can be written in the form (4.53). By the transformation rule (C.23), its density is given by $\frac{1}{\sqrt{|\boldsymbol{\Sigma}|}}\kappa_\alpha(\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{x} - \boldsymbol{\mu}))$. Special instances of the Bessel pdf include:

$$\begin{aligned}
\kappa_2(x) &= \frac{\exp(-\sqrt{2}\,|x|)}{\sqrt{2}} \\
\kappa_4(x) &= \frac{1 + 2\,|x|}{2}\exp(-2\,|x|) \\
\kappa_4(x_1, x_2, x_3) &= \frac{1}{\pi}\exp\left(-2\sqrt{x_1^2 + x_2^2 + x_3^2}\right) \\
\kappa_{d+1}(\boldsymbol{x}) &= \frac{((d+1)/2)^{d/2}\sqrt{\pi}}{(2\pi)^{d/2}\Gamma((d+1)/2)}\exp\left(-\sqrt{d+1}\,\|\boldsymbol{x}\|\right), \quad \boldsymbol{x} \in \mathbb{R}^d.
\end{aligned}$$

Note that k_2 is the (scaled) pdf of the double-exponential or *Laplace* distribution.

(b) Given the data $\tau = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ in $\mathbb{R}^d$, we wish to fit a Bessel pdf to the data by employing the EM algorithm, augmenting the data with the vector $\boldsymbol{S} = [S_1, \ldots, S_n]^\top$ of missing data. We assume that α is known and $\alpha > d$. Show that conditional on τ (and given $\boldsymbol{\theta}$), the missing data vector $\boldsymbol{S}$ has independent components, with $S_i \sim \mathsf{GIG}(\alpha, b_i, (\alpha - d)/2)$, with $b_i := \|\Sigma^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu})\|^2$, $i = 1, \ldots, n$.

(c) At iteration t of the EM algorithm, let $g^{(t)}(\boldsymbol{s}) = g(\boldsymbol{s} \mid \tau, \boldsymbol{\theta}^{(t-1)})$ be the density of the missing data, given the observed data τ and the current parameter guess $\boldsymbol{\theta}^{(t-1)}$. Show that the expected complete-data log-likelihood is given by:

$$Q^{(t)}(\boldsymbol{\theta}) := \mathbb{E}_{g^{(t)}} \ln g(\tau, \boldsymbol{S} \mid \boldsymbol{\theta}) = -\frac{1}{2}\sum_{i=1}^{n} b_i(\boldsymbol{\theta})\, w_i^{(t-1)} + \text{constant}, \tag{4.54}$$

where $b_i(\boldsymbol{\theta}) = \|\Sigma^{-1/2}(\boldsymbol{x}_i - \boldsymbol{\mu})\|^2$ and

$$w_i^{(t-1)} := \frac{\sqrt{\alpha}\,K_{(\alpha-d+2)/2}\left(\sqrt{\alpha\, b_i(\boldsymbol{\theta}^{(t-1)})}\right)}{\sqrt{b_i(\boldsymbol{\theta}^{(t-1)})}\,K_{(\alpha-d)/2}\left(\sqrt{\alpha\, b_i(\boldsymbol{\theta}^{(t-1)})}\right)} - \frac{\alpha - d}{b_i(\boldsymbol{\theta}^{(t-1)})}, \quad i = 1, \ldots, n.$$

(d) From (4.54) derive the M-step of the EM algorithm. That is, show how $\boldsymbol{\theta}^{(t)}$ is updated from $\boldsymbol{\theta}^{(t-1)}$.

14. Consider the ellipsoid $E = \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{x}\boldsymbol{\Sigma}^{-1}\boldsymbol{x} = 1\}$ in (4.42). Let $\mathbf{U}\mathbf{D}^2\mathbf{U}^\top$ be an SVD of $\boldsymbol{\Sigma}$. Show that the linear transformation $\boldsymbol{x} \mapsto \mathbf{U}^\top\mathbf{D}^{-1}\boldsymbol{x}$ maps the points on E onto the unit sphere $\{\boldsymbol{z} \in \mathbb{R}^d : \|\boldsymbol{z}\| = 1\}$.

15. Figure 4.13 shows how the centered "surfboard" data are projected onto the first column of the principal component matrix $\mathbf{U}$. Suppose we project the data instead onto the plane spanned by the first *two* columns of $\mathbf{U}$. What are a and b in the representation $ax_1 + bx_2 = x_3$ of this plane?

16. Figure 4.14 suggests that we can assign each feature vector $\boldsymbol{x}$ in the `iris` data set to one of two clusters, based on the value of $\boldsymbol{u}_1^\top\boldsymbol{x}$, where $\boldsymbol{u}_1$ is the first principal component. Plot the sepal lengths against petal lengths and color the points for which $\boldsymbol{u}_1^\top\boldsymbol{x} < 1.5$ differently to points for which $\boldsymbol{u}_1^\top\boldsymbol{x} \geqslant 1.5$. To which species of iris do these clusters correspond?

CHAPTER 5

REGRESSION

Many supervised learning techniques can be gathered under the name "regression". The purpose of this chapter is to explain the mathematical ideas behind regression models and their practical aspects. We analyze the fundamental linear model in detail, and also discuss nonlinear and generalized linear models.

5.1 Introduction

Francis Galton observed in an article in 1889 that the heights of adult offspring are, on the whole, more "average" than the heights of their parents. Galton interpreted this as a degenerative phenomenon, using the term "regression" to indicate this "return to mediocrity". Nowadays, *regression* refers to a broad class of supervised learning techniques where the aim is to predict a quantitative response (output) variable y via a function $g(\boldsymbol{x})$ of an explanatory (input) vector $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$, consisting of p features, each of which can be continuous or discrete. For instance, regression could be used to predict the birth weight of a baby (the response variable) from the weight of the mother, her socio-economic status, and her smoking habits (the explanatory variables).

REGRESSION

Let us recapitulate the framework of supervised learning established in Chapter 2. The aim is to find a prediction function g that best guesses[1] what the random output Y will be for a random input vector $\boldsymbol{X}$. The joint pdf $f(\boldsymbol{x}, y)$ of $\boldsymbol{X}$ and Y is unknown, but a training set $\tau = \{(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)\}$ is available, which is thought of as the outcome of a random training set $\mathcal{T} = \{(\boldsymbol{X}_1, Y_1), \ldots, (\boldsymbol{X}_n, Y_n)\}$ of iid copies of $(\boldsymbol{X}, Y)$. Once we have selected a loss function $\text{Loss}(y, \widehat{y})$, such as the *squared-error loss*

☞ 19

SQUARED-ERROR LOSS

$$\text{Loss}(y, \widehat{y}) = (y - \widehat{y})^2, \tag{5.1}$$

then the "best" prediction function g is defined as the one that minimizes the *risk* $\ell(g) = \mathbb{E}\,\text{Loss}(Y, g(\boldsymbol{X}))$. We saw in Section 2.2 that for the squared-error loss this optimal prediction function is the conditional expectation

RISK

$$g^*(\boldsymbol{x}) = \mathbb{E}[Y \,|\, \boldsymbol{X} = \boldsymbol{x}].$$

[1] Recall the mnemonic use of "g" for "guess"

As the squared-error loss is the most widely-used loss function for regression, we will adopt this loss function in most of this chapter.

The optimal prediction function g^* has to be learned from the training set τ by minimizing the training loss

$$\ell_\tau(g) = \frac{1}{n}\sum_{i=1}^{n}(y_i - g(\boldsymbol{x}_i))^2 \tag{5.2}$$

over a suitable class of functions $\mathcal{G}$. Note that in the above definition, the training set τ is assumed to be fixed. For a random training set $\mathcal{T}$, we will write the training loss as $\ell_\mathcal{T}(g)$. The function $g_\tau^\mathcal{G}$ that minimizes the training loss is the function we use for prediction — the so-called *learner*. When the function class $\mathcal{G}$ is clear from the context, we drop the superscript in the notation.

LEARNER

☞ 21

As we already saw in (2.2), conditional on $\boldsymbol{X} = \boldsymbol{x}$, the response Y can be written as

$$Y = g^*(\boldsymbol{x}) + \varepsilon(\boldsymbol{x}),$$

where $\mathbb{E}\,\varepsilon(\boldsymbol{x}) = 0$. This motivates a standard modeling assumption in supervised learning, in which the responses $Y_1, \ldots, Y_n$, conditional on the explanatory variables $\boldsymbol{X}_1 = \boldsymbol{x}_1, \ldots, \boldsymbol{X}_n = \boldsymbol{x}_n$, are assumed to be of the form

$$Y_i = g(\boldsymbol{x}_i) + \varepsilon_i, \quad i = 1, \ldots, n,$$

where the $\{\varepsilon_i\}$ are independent with $\mathbb{E}\,\varepsilon_i = 0$ and $\mathbb{V}\mathrm{ar}\,\varepsilon_i = \sigma^2$ for some function $g \in \mathcal{G}$ and variance σ^2. The above model is usually further specified by assuming that g is completely known up to an unknown parameter vector; that is,

$$Y_i = g(\boldsymbol{x}_i\,|\,\boldsymbol{\beta}) + \varepsilon_i, \quad i = 1, \ldots, n. \tag{5.3}$$

While the model (5.3) is described *conditional* on the explanatory variables, it will be convenient to make one further model simplification, and view (5.3) as if the $\{\boldsymbol{x}_i\}$ were *fixed*, while the $\{Y_i\}$ are random.

For the remainder of this chapter, we assume that the training feature vectors $\{\boldsymbol{x}_i\}$ are fixed and only the responses are random; that is, $\mathcal{T} = \{(\boldsymbol{x}_1, Y_1), \ldots, (\boldsymbol{x}_n, Y_n)\}$.

The advantage of the model (5.3) is that the problem of estimating the *function* g from the training data is reduced to the (much simpler) problem of estimating the *parameter vector* $\boldsymbol{\beta}$. An obvious disadvantage is that functions of the form $g(\cdot\,|\,\boldsymbol{\beta})$ may not accurately approximate the true unknown g^*. The remainder of this chapter deals with the analysis of models of the form (5.3). In the important case where the function $g(\cdot\,|\,\boldsymbol{\beta})$ is *linear*, the analysis proceeds through the class of linear models. If, in addition, the error terms $\{\varepsilon_i\}$ are assumed to be *Gaussian*, this analysis can be carried out using the rich theory of normal linear models.

5.2 Linear Regression

The most basic regression model involves a linear relationship between the response and a single explanatory variable. In particular, we have measurements $(x_1, y_1), \ldots, (x_n, y_n)$ that lie approximately on a straight line, as in Figure 5.1.

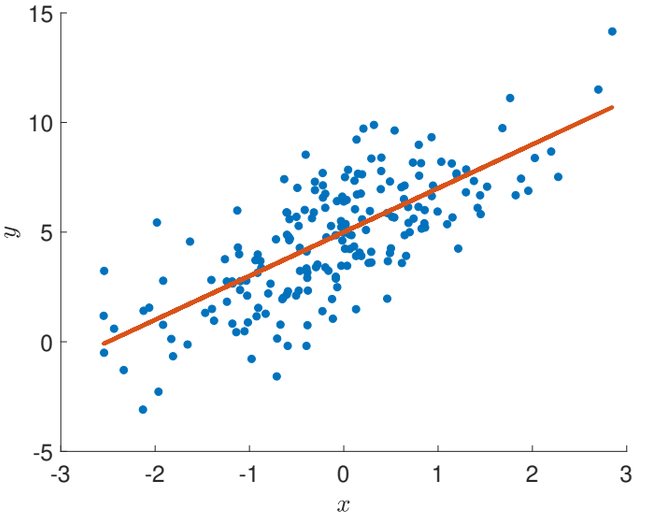


Figure 5.1: Data from a simple linear regression model.

Following the general scheme captured in (5.3), a simple model for these data is that the $\{x_i\}$ are fixed and variables $\{Y_i\}$ are random such that

$$Y_i = \beta_0 + \beta_1 x_i + \varepsilon_i, \quad i = 1, \ldots, n, \tag{5.4}$$

for certain *unknown* parameters β_0 and β_1. The $\{\varepsilon_i\}$ are assumed to be independent with expectation 0 and unknown variance σ^2. The unknown line

$$y = \underbrace{\beta_0 + \beta_1 x}_{g(x|\boldsymbol{\beta})} \tag{5.5}$$

is called the *regression line*. Thus, we view the responses as random variables that would lie exactly on the regression line, were it not for some "disturbance" or "error" term represented by the $\{\varepsilon_i\}$. The extent of the disturbance is modeled by the parameter σ^2. The model in (5.4) is called *simple linear regression*. This model can easily be extended to incorporate more than one explanatory variable, as follows.

REGRESSION LINE

SIMPLE LINEAR REGRESSION MODEL

Definition 5.1: Multiple Linear Regression Model

In a *multiple linear regression model* the response Y depends on a d-dimensional explanatory vector $\boldsymbol{x} = [x_1, \ldots, x_d]^\top$, via the linear relationship

$$Y = \beta_0 + \beta_1 x_1 + \cdots + \beta_d x_d + \varepsilon, \tag{5.6}$$

where $\mathbb{E}\,\varepsilon = 0$ and $\mathbb{V}\mathrm{ar}\,\varepsilon = \sigma^2$.

MULTIPLE LINEAR REGRESSION MODEL

Thus, the data lie approximately on a d-dimensional affine hyperplane

$$y = \underbrace{\beta_0 + \beta_1 x_1 + \cdots + \beta_d x_d}_{g(\boldsymbol{x}\,|\,\boldsymbol{\beta})},$$

where we define $\boldsymbol{\beta} = [\beta_0, \beta_1, \ldots, \beta_d]^\top$. The function $g(\boldsymbol{x}\,|\,\boldsymbol{\beta})$ is linear in $\boldsymbol{\beta}$, but not linear in the feature vector $\boldsymbol{x}$, due to the constant β_0. However, *augmenting* the feature space with the constant 1, the mapping $[1, \boldsymbol{x}^\top]^\top \mapsto g(\boldsymbol{x}\,|\,\boldsymbol{\beta}) := [1, \boldsymbol{x}^\top]\boldsymbol{\beta}$ becomes linear in the feature space and so (5.6) becomes a *linear model* (see Section 2.1). Most software packages for regression include 1 as a feature by default.

☞ 43

Note that in (5.6) we only specified the model for a single pair $(\boldsymbol{x}, Y)$. The model for the training set $\mathcal{T} = \{(\boldsymbol{x}_1, Y_1), \ldots, (\boldsymbol{x}_n, Y_n)\}$ is simply that each Y_i satisfies (5.6) (with $\boldsymbol{x} = \boldsymbol{x}_i$) and that the $\{Y_i\}$ are independent. Setting $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$, we can write the multiple linear regression model for the training data compactly as

$$\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}, \tag{5.7}$$

MODEL MATRIX

where $\boldsymbol{\varepsilon} = [\varepsilon_1, \ldots, \varepsilon_n]^\top$ is a vector of iid copies of ε and $\mathbf{X}$ is the *model matrix* given by

$$\mathbf{X} = \begin{bmatrix} 1 & x_{11} & x_{12} & \cdots & x_{1d} \\ 1 & x_{21} & x_{22} & \cdots & x_{2d} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n1} & x_{n2} & \cdots & x_{nd} \end{bmatrix} = \begin{bmatrix} 1 & \boldsymbol{x}_1^\top \\ 1 & \boldsymbol{x}_2^\top \\ \vdots & \vdots \\ 1 & \boldsymbol{x}_n^\top \end{bmatrix}.$$

■ **Example 5.1 (Multiple Linear Regression Model)** Figure 5.2 depicts a realization of the multiple linear regression model

$$Y_i = x_{i1} + x_{i2} + \varepsilon_i, \quad i = 1, \ldots, 100,$$

where $\varepsilon_1, \ldots, \varepsilon_{100} \sim_{\text{iid}} \mathcal{N}(0, 1/16)$. The fixed feature vectors (vectors of explanatory variables) $\boldsymbol{x}_i = [x_{i1}, x_{i2}]^\top$, $i = 1, \ldots, 100$ lie in the unit square.

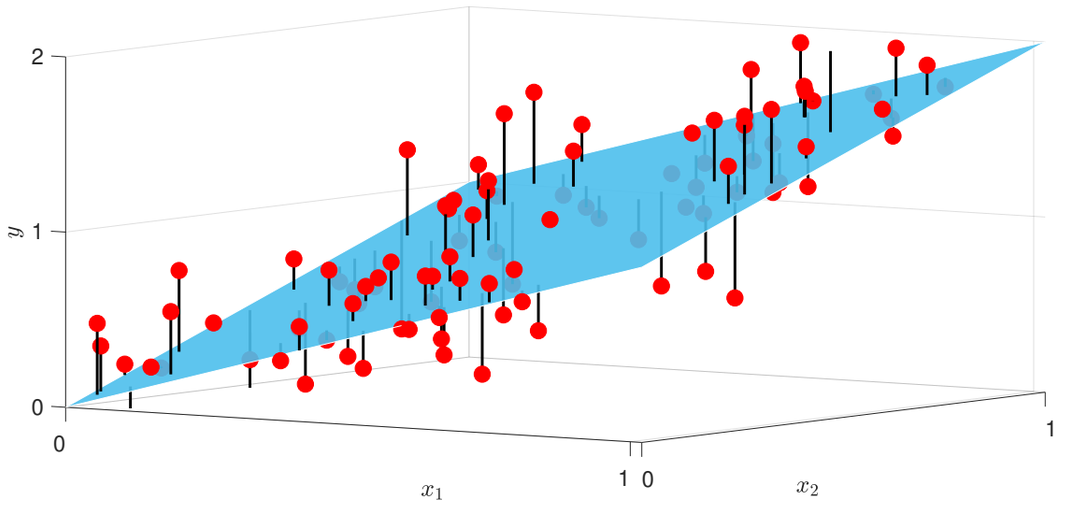


Figure 5.2: Data from a multiple linear regression model.

■

5.3 Analysis via Linear Models

Analysis of data from a linear regression model is greatly simplified through the linear model representation (5.7). In this section we present the main ideas for parameter estimation and model selection for a general linear model of the form

$$\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}, \tag{5.8}$$

where $\mathbf{X}$ is an $n \times p$ matrix, $\boldsymbol{\beta} = [\beta_1, \ldots, \beta_p]^\top$ a vector of p parameters, and $\boldsymbol{\varepsilon} = [\varepsilon_1, \ldots, \varepsilon_n]^\top$ an n-dimensional vector of independent error terms, with $\mathbb{E}\,\varepsilon_i = 0$ and $\mathbb{V}\mathrm{ar}\,\varepsilon_i = \sigma^2$, $i = 1, \ldots, n$. Note that the model matrix $\mathbf{X}$ is assumed to be fixed, and $\boldsymbol{Y}$ and $\boldsymbol{\varepsilon}$ are random. A specific outcome of $\boldsymbol{Y}$ is denoted by $\boldsymbol{y}$ (in accordance with the notation in Section 2.8). ☞ 46

Note that the multiple linear regression model in (5.7) was defined using a different parameterization; in particular, there we used $\boldsymbol{\beta} = [\beta_0, \beta_1, \ldots, \beta_d]^\top$. So, when applying the results in the present section to such models, be aware that $p = d + 1$. Also, in this section a feature vector $\boldsymbol{x}$ includes the constant 1, so that $\mathbf{X}^\top = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$.

5.3.1 Parameter Estimation

The linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$ contains two unknown parameters, $\boldsymbol{\beta}$ and σ^2, which have to be estimated from the training data τ. To estimate $\boldsymbol{\beta}$, we can repeat exactly the same reasoning used in our recurring polynomial regression Example 2.1 as follows. For a linear prediction function $g(\boldsymbol{x}) = \boldsymbol{x}^\top\boldsymbol{\beta}$, the (squared-error) training loss can be written as ☞ 26

$$\ell_\tau(g) = \frac{1}{n}\,\|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2,$$

and the optimal learner g_τ minimizes this quantity, leading to the least-squares estimate $\widehat{\boldsymbol{\beta}}$, which satisfies the normal equations

$$\mathbf{X}^\top\mathbf{X}\,\boldsymbol{\beta} = \mathbf{X}^\top\boldsymbol{y}. \tag{5.9}$$

The corresponding training loss can be taken as an estimate of σ^2; that is,

$$\widehat{\sigma^2} = \frac{1}{n}\,\|\,\boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\,\|^2. \tag{5.10}$$

To justify the latter, note that σ^2 is the second moment of the model errors $\varepsilon_i, i = 1, \ldots, n$, in (5.8) and could be estimated via the method of moments (see Section C.12.1) using the sample average $n^{-1}\sum_i \varepsilon_i^2 = \|\boldsymbol{\varepsilon}\|^2/n = \|\boldsymbol{Y} - \mathbf{X}\boldsymbol{\beta}\|^2/n$, if $\boldsymbol{\beta}$ were known. By replacing $\boldsymbol{\beta}$ with its estimator, we arrive at (5.10). Note that no distributional properties of the $\{\varepsilon_i\}$ were used other than $\mathbb{E}\,\varepsilon_i = 0$ and $\mathbb{V}\mathrm{ar}\,\varepsilon_i = \sigma^2, i = 1, \ldots, n$. The vector $\boldsymbol{e} := \boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}$ is called the vector of *residuals* and approximates the (unknown) vector of model errors $\boldsymbol{\varepsilon}$. The quantity $\|\boldsymbol{e}\|^2 = \sum_{i=1}^n e_i^2$ is called the *residual sum of squares* (RSS). Dividing the RSS by $n - p$ gives an unbiased estimate of σ^2, which we call the estimated *residual squared error* (RSE); see Exercise 12. ☞ 457

RESIDUALS

RESIDUAL SUM OF SQUARES

RESIDUAL SQUARED ERROR

In terms of the notation given in the summary Table 2.1 for supervised learning, we thus have:

☞ 25

1. The (observed) training data is $\tau = \{\mathbf{X}, \boldsymbol{y}\}$.
2. The function class $\mathcal{G}$ is the class of linear functions of $\boldsymbol{x}$; that is $\mathcal{G} = \{g(\cdot\,|\boldsymbol{\beta}) : \boldsymbol{x} \mapsto \boldsymbol{x}^\top\boldsymbol{\beta},\ \boldsymbol{\beta} \in \mathbb{R}^p\}$.
3. The (squared-error) training loss is $\ell_\tau(g(\cdot\,|\boldsymbol{\beta})) = \|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2/n$.
4. The learner g_τ is given by $g_\tau(\boldsymbol{x}) = \boldsymbol{x}^\top\widehat{\boldsymbol{\beta}}$, where $\widehat{\boldsymbol{\beta}} = \operatorname{argmin}_{\boldsymbol{\beta}\in\mathbb{R}^p} \|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2$.
5. The minimal training loss is $\ell_\tau(g_\tau) = \|\boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2/n = \widehat{\sigma^2}$.

5.3.2 Model Selection and Prediction

Even if we restrict the learner to be a linear function, there is still the issue of which explanatory variables (features) to include. While including too few features may result in large *approximation error* (underfitting), including too many may result in large *statistical error* (overfitting). As discussed in Section 2.4, we need to select the features which provide the best tradeoff between the approximation and statistical errors, so that the (expected) generalization risk of the learner is minimized. Depending on how the (expected) generalization risk is estimated, there are a number of strategies for feature selection:

☞ 31

1. Use *test data* $\tau' = (\mathbf{X}', \boldsymbol{y}')$ that are obtained independently from the training data τ, to estimate the generalization risk $\mathbb{E}\,\|Y - g_\tau(\boldsymbol{X})\|^2$ via the test loss (2.7). Then choose the collection of features that minimizes the test loss. When there is an abundance of data, part of the data can be reserved as test data, while the remaining data is used as training data.

☞ 24

2. When there is a limited amount of data, we can use *cross-validation* to estimate the expected generalization risk $\mathbb{E}\,\|Y - g_{\mathcal{T}}(\boldsymbol{X})\|^2$ (where $\mathcal{T}$ is a random training set), as explained in Section 2.5.2. This is then minimized over the set of possible choices for the explanatory variables.

☞ 37

3. When one has to choose between many potential explanatory variables, techniques such as *regularized least-squares* and *lasso regression* become important. Such methods offer another approach to model selection, via the regularization (or homotopy) paths. This will be the topic of Section 6.2 in the next chapter.

☞ 216

4. Rather than using computer-intensive techniques, such as the ones above, one can use *theoretical* estimates of the expected generalization risk, such as the in-sample risk, AIC, and BIC, as in Section 2.5, and minimize this to determine a good set of explanatory variables.

☞ 35

5. All of the above approaches do not assume any distributional properties of the error terms $\{\varepsilon_i\}$ in the linear model, other than that they are independent with expectation 0 and variance σ^2. If, however, they are assumed to have a *normal* (Gaussian) distribution, (that is, $\{\varepsilon_i\} \sim_{\text{iid}} \mathcal{N}(0, \sigma^2)$), then the inclusion and exclusion of variables can

be decided by means of *hypotheses tests*. This is the classical approach to model selection, and will be discussed in Section 5.4. As a consequence of the central limit theorem, one can use the same approach when the error terms are not necessarily normal, provided their variance is finite and the sample size n is large.

6. Finally, when using a Bayesian approach, comparison of two models can be achieved by computing their so-called *Bayes factor* (see Section 2.9).

All of the above strategies can be thought of as specifications of a simple rule formulated by William of Occam, which can be interpreted as:

> *When presented with competing models, choose the simplest one that explains the data.*

This age-old principle, known as *Occam's razor*, is mirrored in a famous quote of Einstein: OCCAM'S RAZOR

> *Everything should be made as simple as possible, but not simpler.*

In linear regression, the number of parameters or predictors is usually a reasonable measure of the simplicity of the model.

5.3.3 Cross-Validation and Predictive Residual Sum of Squares

We start by considering the n-fold cross-validation, also called *leave-one-out cross-validation*, for the linear model (5.8). We partition the data into n data sets, leaving out precisely one observation per data set, which we then predict based on the $n-1$ remaining observations; see Section 2.5.2 for the general case. Let $\widehat{y}_{-i}$ denote the prediction for the i-th observation using all the data except y_i. The error in the prediction, $y_i - \widehat{y}_{-i}$, is called a *predicted residual* — in contrast to an ordinary residual, $e_i = y_i - \widehat{y}_i$, which is the difference between an observation and its fitted value $\widehat{y}_i = g_\tau(\boldsymbol{x}_i)$ obtained using the whole sample. In this way, we obtain the collection of predicted residuals $\{y_i - \widehat{y}_{-i}\}_{i=1}^n$ and summarize them through the *predicted residual sum of squares* (*PRESS*):

LEAVE-ONE-OUT CROSS-VALIDATION

☞ 37

PREDICTED RESIDUAL

PRESS

$$\text{PRESS} = \sum_{i=1}^{n} (y_i - \widehat{y}_{-i})^2.$$

Dividing the PRESS by n gives an estimate of the expected generalization risk.

In general, computing the PRESS is computationally intensive as it involves training and predicting n separate times. For linear models, however, the predicted residuals can be calculated quickly using only the ordinary residuals and the projection matrix $\mathbf{P} = \mathbf{X}\mathbf{X}^+$ onto the linear space spanned by the columns of the model matrix $\mathbf{X}$ (see (2.13)). The i-th diagonal element $\mathbf{P}_{ii}$ of the projection matrix is called the i-th *leverage*, and it can be shown that $0 \leqslant \mathbf{P}_{ii} \leqslant 1$ (see Exercise 10).

☞ 171

☞ 28

LEVERAGE

Theorem 5.1: PRESS for Linear Models

Consider the linear model (5.8), where the $n \times p$ model matrix $\mathbf{X}$ is of full rank. Given an outcome $\boldsymbol{y} = [y_1, \ldots, y_n]^\top$ of $\boldsymbol{Y}$, the fitted values can be obtained as $\widehat{\boldsymbol{y}} = \mathbf{P}\boldsymbol{y}$, where $\mathbf{P} = \mathbf{X}\mathbf{X}^+ = \mathbf{X}(\mathbf{X}^\top\mathbf{X})^{-1}\mathbf{X}^\top$ is the projection matrix. If the leverage value $p_i := \mathbf{P}_{ii} \neq 1$ for all $i = 1, \ldots, n$, then the predicted residual sum of squares can be written as

$$\text{PRESS} = \sum_{i=1}^{n} \left(\frac{e_i}{1 - p_i} \right)^2,$$

where $e_i = y_i - \widehat{y}_i = y_i - (\mathbf{X}\widehat{\boldsymbol{\beta}})_i$ is the i-th residual.

Proof: It suffices to show that the i-th predicted residual can be written as $y_i - \widehat{y}_{-i} = e_i/(1 - p_i)$. Let $\mathbf{X}_{-i}$ denote the model matrix $\mathbf{X}$ with the i-th row, $\boldsymbol{x}_i^\top$, removed, and define $\boldsymbol{y}_{-i}$ similarly. Then, the least-squares estimate for $\boldsymbol{\beta}$ using all but the i-th observation is $\widehat{\boldsymbol{\beta}}_{-i} = (\mathbf{X}_{-i}^\top\mathbf{X}_{-i})^{-1}\mathbf{X}_{-i}^\top\boldsymbol{y}_{-i}$. Writing $\mathbf{X}^\top\mathbf{X} = \mathbf{X}_{-i}^\top\mathbf{X}_{-i} + \boldsymbol{x}_i\boldsymbol{x}_i^\top$, we have by the Sherman–Morrison formula ☞ 373

$$(\mathbf{X}_{-i}^\top\mathbf{X}_{-i})^{-1} = (\mathbf{X}^\top\mathbf{X})^{-1} + \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i\boldsymbol{x}_i^\top(\mathbf{X}^\top\mathbf{X})^{-1}}{1 - \boldsymbol{x}_i^\top(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i},$$

where $\boldsymbol{x}_i^\top(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i = p_i < 1$. Also, $\mathbf{X}_{-i}^\top\boldsymbol{y}_{-i} = \mathbf{X}^\top\boldsymbol{y} - \boldsymbol{x}_i y_i$. Combining all these identities, we have

$$\begin{aligned}
\widehat{\boldsymbol{\beta}}_{-i} &= (\mathbf{X}_{-i}^\top\mathbf{X}_{-i})^{-1}\mathbf{X}_{-i}^\top\boldsymbol{y}_{-i} \\
&= \left((\mathbf{X}^\top\mathbf{X})^{-1} + \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i\boldsymbol{x}_i^\top(\mathbf{X}^\top\mathbf{X})^{-1}}{1 - p_i} \right) (\mathbf{X}^\top\boldsymbol{y} - \boldsymbol{x}_i y_i) \\
&= \widehat{\boldsymbol{\beta}} + \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i\boldsymbol{x}_i^\top\widehat{\boldsymbol{\beta}}}{1 - p_i} - (\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i y_i - \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i p_i y_i}{1 - p_i} \\
&= \widehat{\boldsymbol{\beta}} + \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i\boldsymbol{x}_i^\top\widehat{\boldsymbol{\beta}}}{1 - p_i} - \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i y_i}{1 - p_i} \\
&= \widehat{\boldsymbol{\beta}} - \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i(y_i - \boldsymbol{x}_i^\top\widehat{\boldsymbol{\beta}})}{1 - p_i} = \widehat{\boldsymbol{\beta}} - \frac{(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i e_i}{1 - p_i}.
\end{aligned}$$

It follows that the predicted value for the i-th observation is given by

$$\widehat{y}_{-i} = \boldsymbol{x}_i^\top\widehat{\boldsymbol{\beta}}_{-i} = \boldsymbol{x}_i^\top\widehat{\boldsymbol{\beta}} - \frac{\boldsymbol{x}_i^\top(\mathbf{X}^\top\mathbf{X})^{-1}\boldsymbol{x}_i e_i}{1 - p_i} = \widehat{y}_i - \frac{p_i e_i}{1 - p_i}.$$

Hence, $y_i - \widehat{y}_{-i} = e_i + p_i e_i/(1 - p_i) = e_i/(1 - p_i)$. □

■ **Example 5.2 (Polynomial Regression (cont.))** We return to Example 2.1, where we estimated the generalization risk for various polynomial prediction functions using independent validation data. Instead, let us estimate the expected generalization risk via cross-validation (thus using only the training set) and apply Theorem 5.1 to compute the PRESS. ☞ 26

☞ 174

polyregpress.py

```
import numpy as np
import matplotlib.pyplot as plt

def generate_data(beta , sig, n):
    u = np.random.rand(n, 1)
    y = u ** np.arange(0, 4) @ beta.reshape(4,1) + (
                                sig * np.random.randn(n, 1))
    return u, y

np.random.seed(12)
beta = np.array([[10.0, -140, 400, -250]]).T;
sig=5; n = 10**2;
u,y = generate_data(beta,sig,n)

X = np.ones((n, 1))
K = 12 #maximum number of parameters
press = np.zeros(K+1)
for k in range(1,K):
    if k > 1:
        X = np.hstack((X, u**(k-1))) # add column to matrix
    P = X @ np.linalg.pinv(X) # projection matrix
    e = y - P @ y

    press[k] = np.sum((e/(1-np.diag(P).reshape(n,1)))**2)

plt.plot(press[1:K]/n)
```

The PRESS values divided by $n = 100$ for the constant, linear, quadratic, cubic, and quartic order polynomial regression models are, respectively, $152.487, 56.249, 51.606$, 30.999, and 31.634. Hence, the cubic polynomial regression model has the lowest PRESS, indicating that it has the best predictive performance. ■

5.3.4 In-Sample Risk and Akaike Information Criterion

In Section 2.5.1 we introduced the *in-sample risk* as a measure for the accuracy of the prediction function. To recapitulate, given a fixed data set τ with associated response vector $\boldsymbol{y}$ and $n \times p$ matrix of explanatory variables $\mathbf{X}$, the in-sample risk of a prediction function g is defined as

☞ 35

$$\ell_{\text{in}}(g) := \mathbb{E}_{\mathbf{X}} \operatorname{Loss}(Y, g(\boldsymbol{X})), \tag{5.11}$$

where $\mathbb{E}_{\mathbf{X}}$ signifies that the expectation is taken under a different probability model, in which $\boldsymbol{X}$ takes the values $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ with equal probability, and given $\boldsymbol{X} = \boldsymbol{x}_i$ the random variable Y is drawn from the conditional pdf $f(y \,|\, \boldsymbol{x}_i)$. The difference between the in-sample risk and the training loss is called the *optimism*. For the squared-error loss, Theorem 2.2 expresses the expected optimism of a learner $g_{\mathcal{T}}$ as two times the average covariance between the predicted values and the responses.

☞ 36

If the conditional variance of the error $Y - g^*(\boldsymbol{X})$ given $\boldsymbol{X} = \boldsymbol{x}$ does not depend on $\boldsymbol{x}$, then the expected in-sample risk of a learner g_τ, averaged over all training sets, has a simple expression:

Theorem 5.2: Expected In-Sample Risk for Linear Models

Let $\mathbf{X}$ be the model matrix for a linear model, of dimension $n \times p$. If $\mathbb{V}\mathrm{ar}[Y - g^*(\boldsymbol{X}) \,|\, \boldsymbol{X} = \boldsymbol{x}] =: v^2$ does not depend on $\boldsymbol{x}$, then the expected in-sample risk (with respect to the squared-error loss) for a random learner $g_{\mathcal{T}}$ is given by

$$\mathbb{E}_{\mathbf{X}}\, \ell_{\text{in}}(g_{\mathcal{T}}) = \mathbb{E}_{\mathbf{X}}\, \ell_{\mathcal{T}}(g_{\mathcal{T}}) + \frac{2\ell^* p}{n}, \tag{5.12}$$

where ℓ^* is the irreducible risk.

Proof: The expected optimism is, by definition, $\mathbb{E}_{\mathbf{X}}[\ell_{\text{in}}(g_{\mathcal{T}}) - \ell_{\mathcal{T}}(g_{\mathcal{T}})]$ which, for the squared-error loss, is equal to $2\ell^* p/n$, using exactly the same reasoning as in Example 2.3. Note that here $\ell^* = v^2$. □

Equation (5.12) is the basis of the following model comparison heuristic: Estimate the irreducible risk $\ell^* = v^2$ via $\widehat{v^2}$, using a model with relatively high complexity. Then choose the linear model with the lowest value of

$$\|\boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2 + 2\,\widehat{v^2} p. \tag{5.13}$$

We can also use the Akaike information criterion (AIC) as a heuristic for model comparison. We discussed the AIC in the unsupervised learning setting in Section 4.2, but the arguments used there can also be applied to the supervised case, under the in-sample model for the data. In particular, let $\boldsymbol{Z} = (\boldsymbol{X}, Y)$. We wish to predict the joint density

☞ 122

$$f(z) = f(\boldsymbol{x}, y) := \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{\boldsymbol{x}=\boldsymbol{x}_i\}}\, f(y \,|\, \boldsymbol{x}_i),$$

using a prediction function $g(\boldsymbol{z} \,|\, \boldsymbol{\theta})$ from a family $\mathcal{G} := \{g(\boldsymbol{z} \,|\, \boldsymbol{\theta}), \boldsymbol{\theta} \in \mathbb{R}^q\}$, where

$$g(\boldsymbol{z} \,|\, \boldsymbol{\theta}) = g(\boldsymbol{x}, y \,|\, \boldsymbol{\theta}) := \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{\boldsymbol{x}=\boldsymbol{x}_i\}}\, g_i(y \,|\, \boldsymbol{\theta}).$$

Note that q is the number of parameters (typically larger than p for a linear model with a $n \times p$ design matrix).

Following Section 4.2, the in-sample cross-entropy risk in this case is

$$r(\boldsymbol{\theta}) := -\mathbb{E}_{\mathbf{X}} \ln g(\boldsymbol{Z} \,|\, \boldsymbol{\theta}),$$

and to approximate the optimal parameter $\boldsymbol{\theta}^*$ we minimize the corresponding training loss

$$r_{\tau_n}(\boldsymbol{\theta}) := -\frac{1}{n} \sum_{j=1}^{n} \ln g(\boldsymbol{z}_j \,|\, \boldsymbol{\theta}).$$

The optimal parameter $\widehat{\boldsymbol{\theta}}_n$ for the training loss is thus found by minimizing

$$-\frac{1}{n} \sum_{j=1}^{n} \Big(-\ln n + \ln g_j(y_j \,|\, \boldsymbol{\theta})\Big).$$

That is, it is the maximum likelihood estimate of $\boldsymbol{\theta}$:

$$\widehat{\boldsymbol{\theta}}_n = \operatorname*{argmax}_{\boldsymbol{\theta}} \sum_{i=1}^{n} \ln g_i(y_i \,|\, \boldsymbol{\theta}).$$

Under the assumption that $f = g(\cdot \,|\, \boldsymbol{\theta}^*)$ for some parameter $\boldsymbol{\theta}^*$, we have from Theorem 4.1 that the estimated in-sample generalization risk can be approximated as ☞ 125

$$\mathbb{E}_{\mathbf{X}}\, r(\widehat{\boldsymbol{\theta}}_n) \approx r_{\mathcal{T}_n}(\widehat{\boldsymbol{\theta}}_n) + \frac{q}{n} = \ln n - \frac{1}{n}\sum_{j=1}^{n} \ln g_j(y_j \,|\, \widehat{\boldsymbol{\theta}}_n) + \frac{q}{n}.$$

This leads to the heuristic of selecting the learner $g(\cdot \,|\, \widehat{\boldsymbol{\theta}}_n)$ with the smallest value of the AIC:

$$-2 \sum_{i=1}^{n} \ln g_i(y_i \,|\, \widehat{\boldsymbol{\theta}}_n) + 2q. \tag{5.14}$$

■ **Example 5.3 (Normal Linear Model)** For the normal linear model $Y \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2)$ (see (2.34)), with a p-dimensional vector $\boldsymbol{\beta}$, we have ☞ 46

$$g_i(y_i \,|\, \underbrace{\boldsymbol{\beta}, \sigma^2}_{=\boldsymbol{\theta}}) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{1}{2}\frac{(y_i - \boldsymbol{x}_i^\top \boldsymbol{\beta})^2}{\sigma^2}\right), \quad i = 1, \ldots, n,$$

so that the AIC is

$$n \ln(2\pi) + n \ln \widehat{\sigma}^2 + \frac{\|\boldsymbol{y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2}{\widehat{\sigma}^2} + 2q, \tag{5.15}$$

where $(\widehat{\boldsymbol{\beta}}, \widehat{\sigma}^2)$ is the maximum likelihood estimate and $q = p+1$ is the number of parameters (including σ^2). For model comparison we may remove the $n \ln(2\pi)$ term if all the models are normal linear models. ■

Certain software packages report the AIC without the $n \ln \widehat{\sigma}^2$ term in (5.15). This may lead to sub-optimal model selection if normal models are compared with non-normal ones.

5.3.5 Categorical Features

Suppose that, as described in Chapter 1, the data is given in the form of a spreadsheet or data frame with n rows and $p + 1$ columns, where the first element of row i is the response variable y_i, and the remaining p elements form the vector of explanatory variables $\boldsymbol{x}_i^\top$. When all the explanatory variables (features, predictors) are *quantitative*, then the model matrix $\mathbf{X}$ can be directly read off from the data frame as the $n \times p$ matrix with rows $\boldsymbol{x}_i^\top, i = 1, \ldots, n$.

However, when some explanatory variables are *qualitative* (categorical), such a one-to-one correspondence between data frame and model matrix no longer holds. The solution is to include *indicator* or *dummy* variables.

FACTORIAL EXPERIMENTS
FACTORS
LEVELS

Linear models with continuous responses and categorical explanatory variables often arise in *factorial experiments*. These are controlled statistical experiments in which the aim is to assess how a response variable is affected by one or more *factors* tested at several *levels*. A typical example is an agricultural experiment where one wishes to investigate how the yield of a food crop depends on factors such as location, pesticide, and fertilizer.

■ **Example 5.4 (Crop Yield)** The data in Table 5.1 lists the yield of a food crop for four different crop treatments (e.g., strengths of fertilizer) on four different blocks (plots).

Table 5.1: Crop yield for different treatments and blocks.

	Treatment			
Block	1	2	3	4
1	9.2988	9.4978	9.7604	10.1025
2	8.2111	8.3387	8.5018	8.1942
3	9.0688	9.1284	9.3484	9.5086
4	8.2552	7.8999	8.4859	8.9485

The corresponding data frame, given in Table 5.2, has 16 rows and 3 columns: one column for the crop yield (the response variable), one column for the Treatment, with levels 1, 2, 3, 4, and one column for the Block, also with levels 1, 2, 3, 4. The values 1, 2, 3, and 4 have no quantitative meaning (it does not make sense to take their average, for example) — they merely identify the category of the treatment or block.

Table 5.2: Crop yield data organized as a data frame in standard format.

Yield	Treatment	Block
9.2988	1	1
8.2111	1	2
9.0688	1	3
8.2552	1	4
9.4978	2	1
8.3387	2	2
⋮	⋮	⋮
9.5086	4	3
8.9485	4	4

■

INDICATOR FEATURE

In general, suppose there are r factor (categorical) variables $u_1, \ldots, u_r$, where the j-th factor has p_j mutually exclusive levels, denoted by $1, \ldots, p_j$. In order to include these categorical variables in a linear model, a common approach is to introduce an *indicator feature* $x_{jk} = \mathbb{1}\{u_j = k\}$ for each factor j at level k. Thus, $x_{jk} = 1$ if the value of factor j is k and 0 otherwise. Since $\sum_k \mathbb{1}\{u_j = k\} = 1$, it suffices to consider only $p_j - 1$ of these indicator features for each factor j (this prevents the model matrix from being rank deficient). For a single response Y, the feature vector $\boldsymbol{x}^\top$ is thus a row vector of binary variables

that indicates which levels were observed for each factor. The model assumption is that Y depends in a linear way on the indicator features, apart from an error term. That is,

$$Y = \beta_0 + \sum_{j=1}^{r} \sum_{k=2}^{p_j} \beta_{jk} \underbrace{\mathbb{1}\{u_j = k\}}_{x_{jk}} + \varepsilon,$$

where we have omitted one indicator feature (corresponding to level 1) for each factor j. For independent responses $Y_1, \ldots, Y_n$, where each Y_i corresponds to the factor values $u_{i1}, \ldots, u_{ir}$, let $x_{ijk} = \mathbb{1}\{u_{ij} = k\}$. Then, the linear model for the data becomes

$$Y_i = \beta_0 + \sum_{j=1}^{r} \sum_{k=2}^{p_j} \beta_{jk} x_{ijk} + \varepsilon_i, \tag{5.16}$$

where the $\{\varepsilon_i\}$ are independent with expectation 0 and some variance σ^2. By gathering the β_0 and $\{\beta_{jk}\}$ into a vector $\boldsymbol{\beta}$, and the $\{x_{ijk}\}$ into a matrix $\mathbf{X}$, we have again a linear model of the form (5.8). The model matrix $\mathbf{X}$ has n rows and $1 + \sum_{j=1}^{r}(p_j - 1)$ columns. Using the above convention that the β_{j1} parameters are subsumed in the parameter β_0 (corresponding to the "constant" feature), we can interpret β_0 as a baseline response when using the explanatory vector $\boldsymbol{x}^\top$ for which $x_{j1} = 1$ for all factors $j = 1, \ldots, r$. The other parameters $\{\beta_{jk}\}$ can be viewed as *incremental effects* relative to this baseline effect. For example, β_{12} describes by how much the response is expected to change if level 2 is used instead of level 1 for factor 1.

INCREMENTAL EFFECTS

■ **Example 5.5 (Crop Yield (cont.))** In Example 5.4, the linear model (5.16) has eight parameters: $\beta_0, \beta_{12}, \beta_{13}, \beta_{14}, \beta_{22}, \beta_{23}, \beta_{24}$, and σ^2. The model matrix $\mathbf{X}$ depends on how the crop yields are organized in a vector $\boldsymbol{y}$ and on the ordering of the factors. Let us order $\boldsymbol{y}$ column-wise from Table 5.1, as in $\boldsymbol{y} = [9.2988, 8.2111, 9.0688, 8.2552, 9.4978, \ldots, 8.9485]^\top$, and let Treatment be Factor 1 and Block be Factor 2. Then we can write (5.16) as

$$\boldsymbol{Y} = \underbrace{\begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{C} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{C} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{C} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{C} \end{bmatrix}}_{\mathbf{X}} \underbrace{\begin{bmatrix} \beta_0 \\ \beta_{12} \\ \beta_{13} \\ \beta_{14} \\ \beta_{22} \\ \beta_{23} \\ \beta_{24} \end{bmatrix}}_{\boldsymbol{\beta}} + \boldsymbol{\varepsilon}, \quad \text{where} \quad \mathbf{C} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and with $\mathbf{1} = [1, 1, 1, 1]^\top$ and $\mathbf{0} = [0, 0, 0, 0]^\top$. Estimation of $\boldsymbol{\beta}$ and σ^2, model selection, and prediction can now be carried out in the usual manner for linear models. ■

In the context of factorial experiments, the model matrix is often called the *design matrix*, as it specifies the design of the experiment; e.g., how many replications are taken for each combination of factor levels. The model (5.16) can be extended by adding products of indicator variables as new features. Such features are called *interaction* terms.

DESIGN MATRIX

INTERACTION

5.3.6 Nested Models

NESTED MODELS

Let $\mathbf{X}$ be a $n \times p$ model matrix of the form $\mathbf{X} = [\mathbf{X}_1, \mathbf{X}_2]$, where $\mathbf{X}_1$ and $\mathbf{X}_2$ are model matrices of dimension $n \times k$ and $n \times (p-k)$, respectively. The linear models $\boldsymbol{Y} = \mathbf{X}_1\boldsymbol{\beta}_1 + \boldsymbol{\varepsilon}$ and $\boldsymbol{Y} = \mathbf{X}_2\boldsymbol{\beta}_2 + \boldsymbol{\varepsilon}$ are said to be *nested within* the linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$. This simply means that certain features in $\mathbf{X}$ are ignored in each of the first two models. Note that $\boldsymbol{\beta}, \boldsymbol{\beta}_1$, and $\boldsymbol{\beta}_2$ are parameter vectors of dimension p, k, and $p-k$, respectively. In what follows, we assume that $n \geqslant p$ and that all model matrices are full-rank.

Suppose we wish to assess whether to use the full model matrix $\mathbf{X}$ or the reduced model matrix $\mathbf{X}_1$. Let $\widehat{\boldsymbol{\beta}}$ be the estimate of $\boldsymbol{\beta}$ under the full model (that is, obtained via (5.9)), and let $\widehat{\boldsymbol{\beta}}_1$ denote the estimate of $\boldsymbol{\beta}_1$ for the reduced model. Let $\boldsymbol{Y}^{(2)} = \mathbf{X}\widehat{\boldsymbol{\beta}}$ be the projection of $\boldsymbol{Y}$ onto the space Span($\mathbf{X}$) spanned by the columns of $\mathbf{X}$; and let $\boldsymbol{Y}^{(1)} = \mathbf{X}_1\widehat{\boldsymbol{\beta}}_1$ be the projection of $\boldsymbol{Y}$ onto the space Span($\mathbf{X}_1$) spanned by the columns of $\mathbf{X}_1$ only; see Figure 5.3. In order to decide whether the features in $\mathbf{X}_2$ are needed, we may compare the estimated error terms of the two models, as calculated by (5.10); that is, by the residual sum of squares divided by the number of observations n. If the outcome of this comparison is that there is little difference between the model error for the full and reduced model, then it is appropriate to adopt the reduced model, as it has fewer parameters than the full model, while explaining the data just as well. The comparison is thus between the squared norms $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2$ and $\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2$. Because of the nested nature of the linear models, Span($\mathbf{X}_1$) is a subspace of Span($\mathbf{X}$) and, consequently, the orthogonal projection of $\boldsymbol{Y}^{(2)}$ onto Span($\mathbf{X}_1$) is the same as the orthogonal projection of $\boldsymbol{Y}$ onto Span($\mathbf{X}_1$); that is, $\boldsymbol{Y}^{(1)}$. By Pythagoras' theorem, we thus have the decomposition $\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2 + \|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2 = \|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2$. This is also illustrated in Figure 5.3.

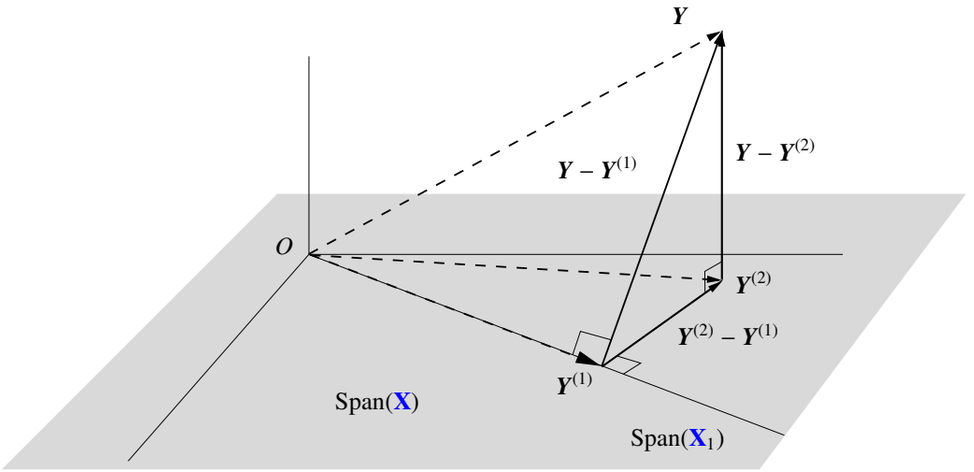


Figure 5.3: The residual sum of squares for the full model corresponds to $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2$ and for the reduced model it is $\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2$. By Pythagoras's theorem, the difference is $\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2$.

The above decomposition can be generalized to more than two model matrices. Suppose that the model matrix can be decomposed into d submatrices: $\mathbf{X} = [\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_d]$, where the matrix $\mathbf{X}_i$ has p_i columns and n rows, $i = 1, \ldots, d$. Thus, the number of columns[2]

[2] As always, we assume the columns are linearly independent.

in the full model matrix is $p = p_1 + \cdots + p_d$. This creates an increasing sequence of "nested" model matrices: $\mathbf{X}_1, [\mathbf{X}_1, \mathbf{X}_2], \ldots, [\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_d]$, from (say) the baseline normal model matrix $\mathbf{X}_1 = \mathbf{1}$ to the full model matrix $\mathbf{X}$. Think of each model matrix corresponding to specific variables in the model.

We follow a similar projection procedure as in Figure 5.3: First project $\boldsymbol{Y}$ onto Span($\mathbf{X}$) to yield the vector $\boldsymbol{Y}^{(d)}$, then project $\boldsymbol{Y}^{(d)}$ onto Span($[\mathbf{X}_1, \ldots, \mathbf{X}_{d-1}]$) to obtain $\boldsymbol{Y}^{(d-1)}$, and so on, until $\boldsymbol{Y}^{(2)}$ is projected onto Span($\mathbf{X}_1$) to yield $\boldsymbol{Y}^{(1)} = \overline{Y}\mathbf{1}$ (in the case that $\mathbf{X}_1 = \mathbf{1}$).

By applying Pythagoras' theorem, the total sum of squares can be decomposed as

$$\underbrace{\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2}_{\text{df}=n-p_1} = \underbrace{\|\boldsymbol{Y} - \boldsymbol{Y}^{(d)}\|^2}_{\text{df}=n-p} + \underbrace{\|\boldsymbol{Y}^{(d)} - \boldsymbol{Y}^{(d-1)}\|^2}_{\text{df}=p_d} + \cdots + \underbrace{\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2}_{\text{df}=p_2}. \tag{5.17}$$

Software packages typically report the sums of squares as well as the corresponding *degrees of freedom* (df): $n - p, p_d, \ldots, p_2$.

DEGREES OF FREEDOM

5.3.7 Coefficient of Determination

To assess how a linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$ compares to the default model $\boldsymbol{Y} = \beta_0\mathbf{1} + \boldsymbol{\varepsilon}$, we can compare the variance of the original data, estimated via $\sum_i (Y_i - \overline{Y})^2/n = \|\boldsymbol{Y} - \overline{Y}\mathbf{1}\|^2/n$, with the variance of the fitted data; estimated via $\sum_i (\widehat{Y}_i - \overline{Y})^2/n = \|\widehat{\boldsymbol{Y}} - \overline{Y}\mathbf{1}\|^2/n$, where $\widehat{\boldsymbol{Y}} = \mathbf{X}\widehat{\boldsymbol{\beta}}$. The sum $\sum_i (Y_i - \overline{Y})^2/n = \|\boldsymbol{Y} - \overline{Y}\mathbf{1}\|^2$ is sometimes called the *total sum of squares* (TSS), and the quantity

TOTAL SUM OF SQUARES

$$R^2 = \frac{\|\widehat{\boldsymbol{Y}} - \overline{Y}\mathbf{1}\|^2}{\|\boldsymbol{Y} - \overline{Y}\mathbf{1}\|^2} \tag{5.18}$$

is called the *coefficient of determination* of the linear model. In the notation of Figure 5.3, $\widehat{\boldsymbol{Y}} = \boldsymbol{Y}^{(2)}$ and $\overline{Y}\mathbf{1} = \boldsymbol{Y}^{(1)}$, so that

COEFFICIENT OF DETERMINATION

$$R^2 = \frac{\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2}{\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2} = \frac{\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2 - \|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2}{\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2} = \frac{\text{TSS} - \text{RSS}}{\text{TSS}}.$$

Note that R^2 lies between 0 and 1. An R^2 value close to 1 indicates that a large proportion of the variance in the data has been explained by the model.

Many software packages also give the *adjusted coefficient of determination*, or simply the adjusted R^2, defined by

ADJUSTED COEFFICIENT OF DETERMINATION

$$R^2_{\text{adjusted}} = 1 - (1 - R^2)\frac{n-1}{n-p}.$$

The regular R^2 is always *non-decreasing* in the number of parameters (see Exercise 15), but this may not indicate better predictive power. The adjusted R^2 compensates for this increase by decreasing the regular R^2 as the number of variables increases. This heuristic adjustment can make it easier to compare the quality of two competing models.

5.4 Inference for Normal Linear Models

So far we have not assumed any distribution for the random vector of errors $\boldsymbol{\varepsilon} = [\varepsilon_1, \ldots, \varepsilon_n]^\top$ in a linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$. When the error terms $\{\varepsilon_i\}$ are assumed to be normally distributed (that is, $\{\varepsilon_i\} \sim_{\text{iid}} \mathcal{N}(0, \sigma^2)$), whole new avenues open up for inference on linear models. In Section 2.8 we already saw that for such *normal linear models*, estimation of $\boldsymbol{\beta}$ and σ^2 can be carried out via maximum likelihood methods, yielding the same estimators from (5.9) and (5.10).

☞ 46

The following theorem lists the properties of these estimators. In particular, it shows that $\widehat{\boldsymbol{\beta}}$ and $\widehat{\sigma^2} n/(n-p)$ are independent and unbiased estimators of $\boldsymbol{\beta}$ and σ^2, respectively.

Theorem 5.3: Properties of the Estimators for a Normal Linear Model

Consider the linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$, with $\boldsymbol{\varepsilon} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I}_n)$, where $\boldsymbol{\beta}$ is a p-dimensional vector of parameters and σ^2 a dispersion parameter. The following results hold.

1. The maximum likelihood estimators $\widehat{\boldsymbol{\beta}}$ and $\widehat{\sigma^2}$ are independent.
2. $\widehat{\boldsymbol{\beta}} \sim \mathcal{N}(\boldsymbol{\beta},\ \sigma^2(\mathbf{X}^\top\mathbf{X})^+)$.
3. $n\widehat{\sigma^2}/\sigma^2 \sim \chi^2_{n-p}$, where $p = \operatorname{rank}(\mathbf{X})$.

☞ 362

Proof: Using the pseudo-inverse (Definition A.2), we can write the random vector $\widehat{\boldsymbol{\beta}}$ as $\mathbf{X}^+\boldsymbol{Y}$, which is a linear transformation of a normal random vector. Consequently, $\widehat{\boldsymbol{\beta}}$ has a multivariate normal distribution; see Theorem C.6. The mean vector and covariance matrix follow from the same theorem:

☞ 437

$$\mathbb{E}\widehat{\boldsymbol{\beta}} = \mathbf{X}^+ \mathbb{E}\boldsymbol{Y} = \mathbf{X}^+\mathbf{X}\boldsymbol{\beta} = \boldsymbol{\beta}$$

and

$$\mathbb{C}\text{ov}(\widehat{\boldsymbol{\beta}}) = \mathbf{X}^+\sigma^2\mathbf{I}_n(\mathbf{X}^+)^\top = \sigma^2(\mathbf{X}^\top\mathbf{X})^+.$$

To show that $\widehat{\boldsymbol{\beta}}$ and $\widehat{\sigma^2}$ are independent, define $\boldsymbol{Y}^{(2)} = \mathbf{X}\widehat{\boldsymbol{\beta}}$. Note that $\boldsymbol{Y}/\sigma$ has a $\mathcal{N}(\boldsymbol{\mu}, \mathbf{I}_n)$ distribution, with expectation vector $\boldsymbol{\mu} = \mathbf{X}\boldsymbol{\beta}/\sigma$. A direct application of Theorem C.10 now shows that $(\boldsymbol{Y} - \boldsymbol{Y}^{(2)})/\sigma$ is independent of $\boldsymbol{Y}^{(2)}/\sigma$. Since $\widehat{\boldsymbol{\beta}} = \mathbf{X}^+\mathbf{X}\widehat{\boldsymbol{\beta}} = \mathbf{X}^+\boldsymbol{Y}^{(2)}$ and $\widehat{\sigma^2} = \|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2/n$, it follows that $\widehat{\sigma^2}$ is independent of $\widehat{\boldsymbol{\beta}}$. Finally, by the same theorem, the random variable $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2/\sigma^2$ has a χ^2_{n-p} distribution, as $\boldsymbol{Y}^{(2)}$ has the same expectation vector as $\boldsymbol{Y}$. □

☞ 440

As a corollary, we see that each estimator $\widehat{\beta_i}$ of β_i has a normal distribution with expectation β_i and variance $\sigma^2\boldsymbol{u}_i^\top\mathbf{X}^+(\mathbf{X}^+)^\top\boldsymbol{u}_i = \sigma^2\|\boldsymbol{u}_i^\top\mathbf{X}^+\|^2$, where $\boldsymbol{u}_i = [0, \ldots, 0, 1, 0, \ldots, 0]^\top$ is the i-th unit vector; in other words, the variance is $\sigma^2[(\mathbf{X}^\top\mathbf{X})^+]_{ii}$.

It is of interest to test whether certain regression parameters β_i are 0 or not, since if $\beta_i = 0$, the i-th explanatory variable has no direct effect on the expected response and so could be removed from the model. A standard procedure is to conduct a hypothesis test (see Section C.14 for a review of hypothesis testing) to test the null hypothesis $H_0 : \beta_i = 0$

☞ 460

against the alternative $H_1 : \beta_i \neq 0$, using the test statistic

$$T = \frac{\widehat{\beta}_i / \|\boldsymbol{u}_i^\top \mathbf{X}^+\|}{\sqrt{\text{RSE}}}, \tag{5.19}$$

where RSE is the residual squared error; that is $\text{RSE} = \text{RSS}/(n-p)$. This test statistic has a t_{n-p} distribution under H_0. To see this, write $T = Z/\sqrt{V/(n-p)}$, with

$$Z = \frac{\widehat{\beta}_i}{\sigma\|\boldsymbol{u}_i^\top \mathbf{X}^+\|} \quad \text{and} \quad V = n\,\widehat{\sigma^2}/\sigma^2.$$

Then, by Theorem 5.3, $Z \sim \mathcal{N}(0,1)$ under H_0, $V \sim \chi^2_{n-p}$, and Z and V are independent. The result now follows directly from Corollary C.1. ☞ 441

5.4.1 Comparing Two Normal Linear Models

Suppose we have the following normal linear model for data $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$:

$$\boldsymbol{Y} = \underbrace{\mathbf{X}_1\boldsymbol{\beta}_1 + \mathbf{X}_2\boldsymbol{\beta}_2}_{\mathbf{X}\boldsymbol{\beta}} + \boldsymbol{\varepsilon}, \quad \boldsymbol{\varepsilon} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_n), \tag{5.20}$$

where $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2$ are unknown vectors of dimension k and $p-k$, respectively; and $\mathbf{X}_1$ and $\mathbf{X}_2$ are full-rank model matrices of dimensions $n \times k$ and $n \times (p-k)$, respectively. Above we implicitly defined $\mathbf{X} = [\mathbf{X}_1, \mathbf{X}_2]$ and $\boldsymbol{\beta}^\top = [\boldsymbol{\beta}_1^\top, \boldsymbol{\beta}_2^\top]$. Suppose we wish to test the hypothesis $H_0 : \boldsymbol{\beta}_2 = \mathbf{0}$ against $H_1 : \boldsymbol{\beta}_2 \neq \mathbf{0}$. Following Section 5.3.6, the idea is to compare the residual sum of squares for both models, expressed as $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2$ and $\|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2$. Using Pythagoras' theorem we saw that $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2 - \|\boldsymbol{Y} - \boldsymbol{Y}^{(1)}\|^2 = \|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2$, and so it makes sense to base the decision whether to retain or reject H_0 on the basis of the quotient of $\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2$ and $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2$. This leads to the following test statistics.

Theorem 5.4: Test Statistic for Comparing Two Normal Linear Models

For the model (5.20), let $\boldsymbol{Y}^{(2)}$ and $\boldsymbol{Y}^{(1)}$ be the projections of $\boldsymbol{Y}$ onto the space spanned by the p columns of $\mathbf{X}$ and the k columns of $\mathbf{X}_1$, respectively. Then under $H_0 : \boldsymbol{\beta}_2 = \mathbf{0}$ the test statistic

$$T = \frac{\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2/(p-k)}{\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2/(n-p)} \tag{5.21}$$

has an $\mathsf{F}(p-k, n-p)$ distribution.

Proof: Define $\boldsymbol{X} := \boldsymbol{Y}/\sigma$ with expectation $\boldsymbol{\mu} := \mathbf{X}\boldsymbol{\beta}/\sigma$, and $\boldsymbol{X}_j := \boldsymbol{Y}^{(j)}/\sigma$ with expectation $\boldsymbol{\mu}_j$, $j = k, p$. Note that $\boldsymbol{\mu}_p = \boldsymbol{\mu}$ and, under H_0, $\boldsymbol{\mu}_k = \boldsymbol{\mu}_p$. We can directly apply Theorem C.10 to find that $\|\boldsymbol{Y} - \boldsymbol{Y}^{(2)}\|^2/\sigma^2 = \|\boldsymbol{X} - \boldsymbol{X}_p\|^2 \sim \chi^2_{n-p}$ and, under H_0, $\|\boldsymbol{Y}^{(2)} - \boldsymbol{Y}^{(1)}\|^2/\sigma^2 = \|\boldsymbol{X}_p - \boldsymbol{X}_k\|^2 \sim \chi^2_{p-k}$. Moreover, these random variables are independent of each other. The proof is completed by applying Theorem C.11. □ ☞ 440

Note that H_0 is rejected for large values of T. The testing procedure thus proceeds as follows:

1. Compute the outcome, t say, of the test statistic T in (5.21).
2. Evaluate the P-value $\mathbb{P}(T \geqslant t)$, with $T \sim \mathsf{F}(p-k, n-p)$.
3. Reject H_0 if this P-value is too small, say less than 0.05.

For nested models $[\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_i]$, $i = 1, 2, \ldots, d$, as in Section 5.3.6, the F test statistic in Theorem 5.4 can now be used to test whether certain $\mathbf{X}_i$ are needed or not. In particular, software packages will report the outcomes of

☞ 183

$$F_i = \frac{\|\boldsymbol{Y}^{(i)} - \boldsymbol{Y}^{(i-1)}\|^2 / p_i}{\|\boldsymbol{Y} - \boldsymbol{Y}^{(d)}\|^2 / (n-p)}, \tag{5.22}$$

in the order $i = 2, 3, \ldots, d$. Under the null hypothesis that $\boldsymbol{Y}^{(i)}$ and $\boldsymbol{Y}^{(i-1)}$ have the same expectation (that is, adding $\mathbf{X}_i$ to $\mathbf{X}_{i-1}$ has no additional effect on reducing the approximation error), the test statistic F_i has an $\mathsf{F}(p_i, n-p)$ distribution, and the corresponding P-values quantify the strength of the decision to include an additional variable in the model or not. This procedure is called *analysis of variance* (ANOVA).

ANALYSIS OF VARIANCE

Note that the output of an ANOVA table depends on the order in which the variables are considered.

■ **Example 5.6 (Crop Yield (cont.))** We continue Examples 5.4 and 5.5. Decompose the linear model as

$$\boldsymbol{Y} = \underbrace{\begin{bmatrix}1\\1\\1\\1\end{bmatrix}}_{\mathbf{X}_1} \underbrace{\beta_0}_{\beta_1} + \underbrace{\begin{bmatrix}0&0&0\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}}_{\mathbf{X}_2} \underbrace{\begin{bmatrix}\beta_{12}\\\beta_{13}\\\beta_{14}\end{bmatrix}}_{\boldsymbol{\beta}_2} + \underbrace{\begin{bmatrix}\mathbf{C}\\\mathbf{C}\\\mathbf{C}\\\mathbf{C}\end{bmatrix}}_{\mathbf{X}_3} \underbrace{\begin{bmatrix}\beta_{22}\\\beta_{23}\\\beta_{24}\end{bmatrix}}_{\boldsymbol{\beta}_3} + \boldsymbol{\varepsilon}.$$

Is the crop yield dependent on treatment levels as well as blocks? We first test whether we can remove Block as a factor in the model against it playing a significant role in explaining the crop yields. Specifically, we test $\boldsymbol{\beta}_3 = \mathbf{0}$ versus $\boldsymbol{\beta}_3 \neq \mathbf{0}$ using Theorem 5.4. Now the vector $\boldsymbol{Y}^{(2)}$ is the projection of $\boldsymbol{Y}$ onto the $(p = 7)$-dimensional space spanned by the columns of $\mathbf{X} = [\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3]$; and $\boldsymbol{Y}^{(1)}$ is the projection of $\boldsymbol{Y}$ onto the $(k = 4)$-dimensional space spanned by the columns of $\mathbf{X}_{12} := [\mathbf{X}_1, \mathbf{X}_2]$. The test statistic, T_{12} say, under H_0 has an $\mathsf{F}(3, 9)$ distribution.

The Python code below calculates the outcome of the test statistic T_{12} and the corresponding P-value. We find $t_{12} = 34.9998$, which gives a P-value 2.73×10^{-5}. This shows that the block effects are extremely important for explaining the data.

Using the extended model (including the block effects), we can test whether $\boldsymbol{\beta}_2 = \mathbf{0}$ or not; that is, whether the treatments have a significant effect on the crop yield in the presence of the Block factor. This is done in the last six lines of the code below. The outcome of

the test statistic is 4.4878, with a P-value of 0.0346. By including the block effects, we effectively reduce the uncertainty in the model and are able to more accurately assess the effects of the treatments, to conclude that the treatment seems to have an effect on the crop yield. A closer look at the data shows that within each block (row) the crop yield roughly increases with the treatment level.

crop.py

```
import numpy as np
from scipy.stats import f
from numpy.linalg import lstsq, norm

yy = np.array([9.2988, 9.4978, 9.7604, 10.1025,
      8.2111, 8.3387, 8.5018,  8.1942,
      9.0688, 9.1284, 9.3484,  9.5086,
      8.2552, 7.8999, 8.4859,  8.9485]).reshape(4,4).T

nrow, ncol = yy.shape[0], yy.shape[1]
n = nrow * ncol
y = yy.reshape(16,)
X_1 = np.ones((n,1))

KM = np.kron(np.eye(ncol),np.ones((nrow,1)))
KM[:,0]
X_2 = KM[:,1:ncol]
IM = np.eye(nrow)
C = IM[:,1:nrow]

X_3 = np.vstack((C, C))
X_3 = np.vstack((X_3, C))
X_3 = np.vstack((X_3, C))

X = np.hstack((X_1,X_2))
X = np.hstack((X,X_3))

p = X.shape[1] #number of parameters in full model
betahat = lstsq(X, y,rcond=None)[0]  #estimate under the full model

ym = X @ betahat

X_12 = np.hstack((X_1, X_2)) #omitting the block effect
k = X_12.shape[1] #number of parameters in reduced model
betahat_12 = lstsq(X_12, y,rcond=None)[0]
y_12 = X_12 @ betahat_12
T_12=(n-p)/(p-k)*(norm(y-y_12)**2 -  norm(y-ym)**2)/norm(y-ym)**2
pval_12 = 1 - f.cdf(T_12,p-k,n-p)

X_13 = np.hstack((X_1, X_3)) #omitting the treatment effect
k = X_13.shape[1] #number of parameters in reduced model
betahat_13 = lstsq(X_13, y,rcond=None)[0]
y_13 = X_13 @ betahat_13
T_13=(n-p)/(p-k)*(norm(y-y_13)**2 - norm(y-ym)**2)/norm(y-ym)**2
pval_13 = 1 - f.cdf(T_13,p-k,n-p)
```

5.4.2 Confidence and Prediction Intervals

As in all supervised learning settings, linear regression is most useful when we wish to predict how a new response variable will behave on the basis of a new explanatory vector $\boldsymbol{x}$. For example, it may be difficult to measure the response variable, but by knowing the estimated regression line and the value for $\boldsymbol{x}$, we will have a reasonably good idea what Y or the expected value of Y is going to be.

Thus, consider a new $\boldsymbol{x}$ and let $Y \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2)$, with $\boldsymbol{\beta}$ and σ^2 unknown. First we are going to look at the *expected* value of Y, that is $\mathbb{E}Y = \boldsymbol{x}^\top \boldsymbol{\beta}$. Since $\boldsymbol{\beta}$ is unknown, we do not know $\mathbb{E}Y$ either. However, we can estimate it via the estimator $\widehat{Y} = \boldsymbol{x}^\top \widehat{\boldsymbol{\beta}}$, where $\widehat{\boldsymbol{\beta}} \sim \mathcal{N}(\boldsymbol{\beta},\ \sigma^2(\mathbf{X}^\top \mathbf{X})^+)$, by Theorem 5.3. Being linear in the components of $\boldsymbol{\beta}$, $\widehat{Y}$ therefore has a normal distribution with expectation $\boldsymbol{x}^\top \boldsymbol{\beta}$ and variance $\sigma^2 \|\boldsymbol{x}^\top \mathbf{X}^+\|^2$. Let $Z \sim \mathcal{N}(0,1)$ be the standardized version of $\widehat{Y}$ and $V = \|\boldsymbol{Y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2/\sigma^2 \sim \chi^2_{n-p}$. Then the random variable

$$T := \frac{(\boldsymbol{x}^\top \widehat{\boldsymbol{\beta}} - \boldsymbol{x}^\top \boldsymbol{\beta}) \,/\, \|\boldsymbol{x}^\top \mathbf{X}^+\|}{\|\boldsymbol{Y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\| \,/\sqrt{(n-p)}} = \frac{Z}{\sqrt{V/(n-p)}} \tag{5.23}$$

☞ 441

has, by Corollary C.1, a t_{n-p} distribution. After rearranging the identity $\mathbb{P}(|T| \leqslant t_{n-p;1-\alpha/2}) = 1-\alpha$, where $t_{n-p;1-\alpha/2}$ is the $(1-\alpha/2)$ quantile of the t_{n-p} distribution, we arrive at the stochastic *confidence interval*

CONFIDENCE INTERVAL

$$\boldsymbol{x}^\top \widehat{\boldsymbol{\beta}} \pm t_{n-p;1-\alpha/2} \sqrt{\mathrm{RSE}}\, \|\boldsymbol{x}^\top \mathbf{X}^+\|, \tag{5.24}$$

where we have identified $\|\boldsymbol{Y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2/(n-p)$ with RSE. This confidence interval quantifies the uncertainty in the learner (regression surface).

PREDICTION INTERVAL

A *prediction interval* for a new response Y is different from a confidence interval for $\mathbb{E}Y$. Here the idea is to construct an interval such that Y lies in this interval with a certain guaranteed probability. Note that now we have *two* sources of variation:

1. $Y \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2)$ itself is a random variable.

2. Estimating $\boldsymbol{x}^\top \boldsymbol{\beta}$ via $\widehat{Y}$ brings another source of variation.

We can construct a $(1-\alpha)$ prediction interval, by finding two random bounds such that the random variable Y lies between these bounds with probability $1-\alpha$. We can reason as follows. Firstly, note that $Y \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2)$ and $\widehat{Y} \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2 \|\boldsymbol{x}^\top \mathbf{X}^+\|^2)$ are independent. It follows that $Y - \widehat{Y}$ has a normal distribution with expectation 0 and variance

$$\sigma^2(1 + \|\boldsymbol{x}^\top \mathbf{X}^+\|^2). \tag{5.25}$$

Secondly, letting $Z \sim \mathcal{N}(0,1)$ be the standardized version of $Y - \widehat{Y}$, and repeating the steps used for the construction of the confidence interval (5.24), we arrive at the prediction interval

$$\boldsymbol{x}^\top \widehat{\boldsymbol{\beta}} \pm t_{n-p;1-\alpha/2} \sqrt{\mathrm{RSE}} \sqrt{1 + \|\boldsymbol{x}^\top \mathbf{X}^+\|^2}. \tag{5.26}$$

This prediction interval captures the uncertainty from an as-yet-unobserved response as well as the uncertainty in the parameters of the regression model itself.

■ **Example 5.7 (Confidence Limits in Simple Linear Regression)** The following program draws $n = 100$ samples from a simple linear regression model with parameters $\boldsymbol{\beta} = [6, 13]^\top$ and $\sigma = 2$, where the x-coordinates are evenly spaced on the interval $[0, 1]$. The parameters are estimated in the third block of the code. Estimates for $\boldsymbol{\beta}$ and σ are $[6.03, 13.09]^\top$ and $\widehat{\sigma} = 1.60$, respectively. The program then proceeds by calculating the 95% numeric confidence and prediction intervals for various values of the explanatory variable. Figure 5.4 shows the results.

confpred.py

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import t
from  numpy.linalg import inv, lstsq, norm
np.random.seed(123)

n = 100
x = np.linspace(0.01,1,100).reshape(n,1)
# parameters
beta = np.array([6,13])
sigma = 2
Xmat = np.hstack((np.ones((n,1)), x)) #design matrix
y = Xmat @ beta + sigma*np.random.randn(n)

# solve the normal equations
betahat = lstsq(Xmat, y,rcond=None)[0]
# estimate for sigma
sqMSE = norm(y - Xmat @ betahat)/np.sqrt(n-2)

tquant = t.ppf(0.975,n-2) # 0.975 quantile
ucl = np.zeros(n) #upper conf. limits
lcl = np.zeros(n) #lower conf. limits
upl = np.zeros(n)
lpl = np.zeros(n)
rl = np.zeros(n)  # (true) regression line
u = 0

for i in range(n):
    u = u + 1/n;
    xvec = np.array([1,u])
    sqc = np.sqrt(xvec.T @ inv(Xmat.T @ Xmat) @ xvec)
    sqp = np.sqrt(1 + xvec.T @ inv(Xmat.T @ Xmat) @ xvec)
    rl[i] = xvec.T @ beta;
    ucl[i] = xvec.T @ betahat + tquant*sqMSE*sqc;
    lcl[i] = xvec.T @ betahat - tquant*sqMSE*sqc;
    upl[i] = xvec.T @ betahat + tquant*sqMSE*sqp;
    lpl[i] = xvec.T @ betahat - tquant*sqMSE*sqp;

plt.plot(x,y, '.')
plt.plot(x,rl,'b')
plt.plot(x,ucl,'k:')
plt.plot(x,lcl,'k:')
plt.plot(x,upl,'r--')
plt.plot(x,lpl,'r--')
```

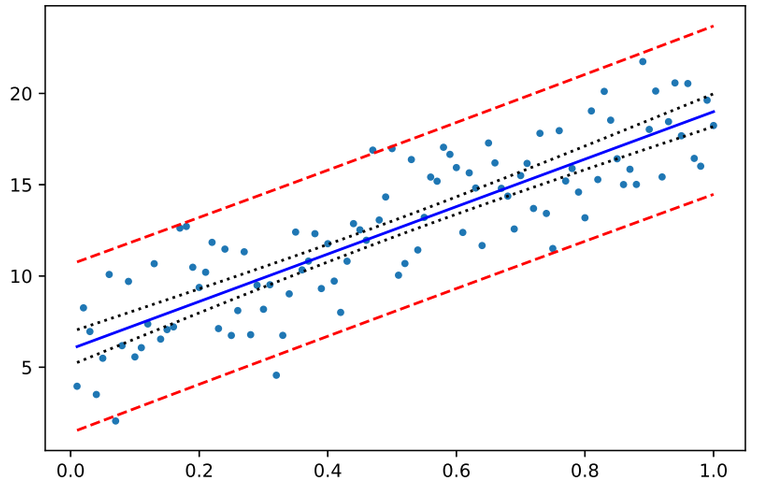


Figure 5.4: The true regression line (blue, solid) and the upper and lower 95% prediction curves (red, dashed) and confidence curves (dotted). ■

5.5 Nonlinear Regression Models

So far we have been mostly dealing with linear regression models, in which the prediction function is of the form $g(\boldsymbol{x}\,|\,\boldsymbol{\beta}) = \boldsymbol{x}^\top\boldsymbol{\beta}$. In this section we discuss some strategies for handling general prediction functions $g(\boldsymbol{x}\,|\,\boldsymbol{\beta})$, where the functional form is known up to an unknown parameter vector $\boldsymbol{\beta}$. So the regression model becomes

$$Y_i = g(\boldsymbol{x}_i\,|\,\boldsymbol{\beta}) + \varepsilon_i, \quad i = 1, \ldots, n, \tag{5.27}$$

where $\varepsilon_1, \ldots, \varepsilon_n$ are independent with expectation 0 and unknown variance σ^2. The model can be further specified by assuming that the error terms have a normal distribution.

Table 5.3 gives some common examples of nonlinear prediction functions for data taking values in $\mathbb{R}$.

Table 5.3: Common nonlinear prediction functions for one-dimensional data.

Name	$g(x\,\|\,\boldsymbol{\beta})$	$\boldsymbol{\beta}$
Exponential	$a\,\mathrm{e}^{bx}$	a, b
Power law	$a\,x^b$	a, b
Logistic	$(1 + \mathrm{e}^{a+bx})^{-1}$	a, b
Weibull	$1 - \exp(-x^b/a)$	a, b
Polynomial	$\sum_{k=0}^{p-1} \beta_k x^k$	p, $\{\beta_k\}_{k=0}^{p-1}$

The logistic and polynomial prediction functions in Table 5.3 can be readily generalized to higher dimensions. For example, for $\boldsymbol{x} \in \mathbb{R}^2$ a general second-order polynomial prediction function is of the form

$$g(\boldsymbol{x}\,|\,\boldsymbol{\beta}) = \beta_0 + \beta_1\,x_1 + \beta_2\,x_2 + \beta_{11}\,x_1^2 + \beta_{22}\,x_2^2 + \beta_{12}\,x_1\,x_2. \tag{5.28}$$

This function can be viewed as a second-order approximation to a general smooth prediction function $g(x_1, x_2)$; see also Exercise 4. Polynomial regression models are also called *response surface* models. The generalization of the above logistic prediction to $\mathbb{R}^d$ is

RESPONSE SURFACE MODEL

$$g(\boldsymbol{x}\,|\,\boldsymbol{\beta}) = (1 + \mathrm{e}^{-\boldsymbol{x}^\top \boldsymbol{\beta}})^{-1}. \tag{5.29}$$

This function will make its appearance in Section 5.7 and later on in Chapters 7 and 9.

The first strategy for performing regression with nonlinear prediction functions is to extend the feature space to obtain a simpler (ideally linear) prediction function in the extended feature space. We already saw an application of this strategy in Example 2.1 for the polynomial regression model, where the original feature u was extended to the feature vector $\boldsymbol{x} = [1, u, u^2, \ldots, u^{p-1}]^\top$, yielding a linear prediction function. In a similar way, the right-hand side of the polynomial prediction function in (5.28) can be viewed as a linear function of the extended feature vector $\boldsymbol{\phi}(\boldsymbol{x}) = [1, x_1, x_2, x_1^2, x_2^2, x_1 x_2]^\top$. The function $\boldsymbol{\phi}$ is called a *feature map*.

☞ 26

FEATURE MAP

The second strategy is to transform the response variable y and possibly also the explanatory variable $\boldsymbol{x}$ such that the transformed variables $\widetilde{y}, \widetilde{\boldsymbol{x}}$ are related in a simpler (ideally linear) way. For example, for the exponential prediction function $y = a\,\mathrm{e}^{-bx}$, we have $\ln y = \ln a - bx$, which is a linear relation between $\ln y$ and $[1, x]^\top$.

■ **Example 5.8 (Chlorine)** Table 5.4 lists the free chlorine concentration (in mg per liter) in a swimming pool, recorded every 8 hours for 4 days. A simple chemistry-based model for the chlorine concentration y as a function of time t is $y = a\,\mathrm{e}^{-b\,t}$, where a is the initial concentration and $b > 0$ is the reaction rate.

Table 5.4: Chlorine concentration (in mg/L) as a function of time (hours).

Hours	Concentration	Hours	Concentration
0	1.0056	56	0.3293
8	0.8497	64	0.2617
16	0.6682	72	0.2460
24	0.6056	80	0.1839
32	0.4735	88	0.1867
40	0.4745	96	0.1688
48	0.3563		

The exponential relationship $y = a\,\mathrm{e}^{-bt}$ suggests that a log transformation of y will result in a *linear* relationship between $\ln y$ and the feature vector $[1, t]^\top$. Thus, if for some given data $(t_1, y_1), \ldots, (t_n, y_n)$, we plot $(t_1, \ln y_1), \ldots, (t_n, \ln y_n)$, these points should approximately lie on a straight line, and hence the simple linear regression model applies. The left panel of Figure 5.5 illustrates that the transformed data indeed lie approximately on a straight line. The estimated regression line is also drawn here. The intercept and slope are $\beta_0 = -0.0555$ and $\beta_1 = -0.0190$ here. The original (non-transformed) data is shown in the right panel of Figure 5.5, along with the fitted curve $y = \widehat{a}\,\mathrm{e}^{-\widehat{b}t}$, where $\widehat{a} = \exp(\widehat{\beta}_0) = 0.9461$ and $\widehat{b} = -\widehat{\beta}_1 = 0.0190$.

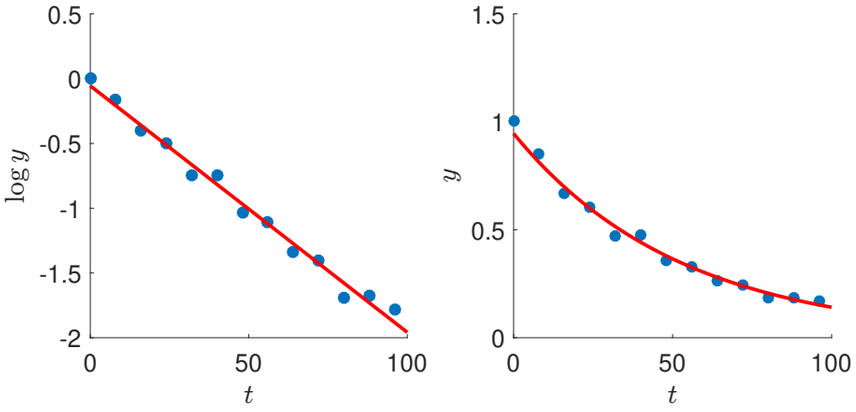


Figure 5.5: The chlorine concentration seems to have an exponential decay. ■

Recall that for a general regression problem the learner $g_\tau(\boldsymbol{x})$ for a given training set τ is obtained by minimizing the training (squared-error) loss

$$\ell_\tau(g(\cdot\,|\boldsymbol{\beta})) = \frac{1}{n}\sum_{i=1}^{n}(y_i - g(\boldsymbol{x}_i\,|\boldsymbol{\beta}))^2. \tag{5.30}$$

The third strategy for regression with nonlinear prediction functions is to directly minimize (5.30) by any means possible, as illustrated in the next example.

■ **Example 5.9 (Hougen Function)** In [7] the reaction rate y of a certain chemical reaction is posited to depend on three input variables: quantities of hydrogen x_1, n-pentane x_2, and isopentane x_3. The functional relationship is given by the *Hougen* function:

$$y = \frac{\beta_1\, x_2 - x_3/\beta_5}{1 + \beta_2\, x_1 + \beta_3\, x_2 + \beta_4\, x_3},$$

where $\beta_1, \ldots, \beta_5$ are the unknown parameters. The objective is to estimate the model parameters $\{\beta_i\}$ from the data, as given in Table 5.5.

Table 5.5: Data for the Hougen function.

x_1	x_2	x_3	y	x_1	x_2	x_3	y
470	300	10	8.55	470	190	65	4.35
285	80	10	3.79	100	300	54	13.00
470	300	120	4.82	100	300	120	8.50
470	80	120	0.02	100	80	120	0.05
470	80	10	2.75	285	300	10	11.32
100	190	10	14.39	285	190	120	3.13
100	80	65	2.54				

The estimation is carried out via the least-squares method. The objective function to minimize is thus

$$\ell_\tau(g(\cdot\,|\boldsymbol{\beta})) = \frac{1}{13}\sum_{i=1}^{13}\left(y_i - \frac{\beta_1\, x_{i2} - x_{i3}/\beta_5}{1 + \beta_2\, x_{i1} + \beta_3\, x_{i2} + \beta_4\, x_{i3}}\right)^2, \tag{5.31}$$

where the $\{y_i\}$ and $\{x_{ij}\}$ are given in Table 5.5.

This is a highly nonlinear optimization problem, for which standard nonlinear least-squares methods do not work well. Instead, one can use global optimization methods such as CE and SCO (see Sections 3.4.2 and 3.4.3). Using the CE method, we found the minimal value 0.02299 for the objective function, which is attained at

☞ 416

☞ 100

$$\widehat{\boldsymbol{\beta}} = [1.2526,\ 0.0628,\ 0.0400,\ 0.1124,\ 1.1914]^\top.$$

■

5.6 Linear Models in Python

In this section we describe how to define and analyze linear models using Python and the data science module **statsmodels**. We encourage the reader to regularly refer back to the theory in the preceding sections of this chapter, so as to avoid using Python merely as a black box without understanding the underlying principles. To run the code start by importing the following code snippet:

```
import matplotlib.pyplot as plt
import pandas as pd
import statsmodels.api as sm
from statsmodels.formula.api import ols
```

5.6.1 Modeling

Although specifying a normal[3] linear model in Python is relatively easy, it requires some subtlety. The main thing to realize is that Python treats quantitative and qualitative (that is, categorical) explanatory variables differently. In **statsmodels**, ordinary least-squares linear models are specified via the function **ols** (short for ordinary least-squares). The main argument of this function is a formula of the form

$$\mathtt{y} \sim \mathtt{x1} + \mathtt{x2} + \cdots + \mathtt{xd}, \tag{5.32}$$

where `y` is the name of the response variable and `x1`, ..., `xd` are the names of the explanatory variables. If all variables are *quantitative*, this describes the linear model

$$Y_i = \beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \cdots + \beta_d x_{id} + \varepsilon_i, \quad i = 1, \ldots, n, \tag{5.33}$$

where x_{ij} is the j-th explanatory variable for the i-th observation and the errors ε_i are independent normal random variables such that $\mathbb{E}\varepsilon_i = 0$ and $\mathbb{V}\mathrm{ar}\,\varepsilon_i = \sigma^2$. Or, in matrix form: $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$, with

$$\boldsymbol{Y} = \begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} 1 & x_{11} & \cdots & x_{1d} \\ 1 & x_{21} & \cdots & x_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n1} & \cdots & x_{nd} \end{bmatrix}, \quad \boldsymbol{\beta} = \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_d \end{bmatrix}, \text{ and } \boldsymbol{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{bmatrix}.$$

[3] For the rest of this section, we assume all linear models to be normal.

Thus, the first column is always taken as an "intercept" parameter, unless otherwise specified. To remove the intercept term, add `-1` to the `ols` formula, as in `ols('y~x-1')`.

For any linear model, the model matrix can be retrieved via the construction:

```
model_matrix = pd.DataFrame(model.exog,columns=model.exog_names)
```

Let us look at some examples of linear models. In the first model the variables `x1` and `x2` are both considered (by Python) to be quantitative.

```
myData = pd.DataFrame({'y' : [10,9,4,2,4,9],
    'x1' : [7.4,1.2,3.1,4.8,2.8,6.5],
    'x2' : [1,1,2,2,3,3]})
mod = ols("y~x1+x2", data=myData)
mod_matrix = pd.DataFrame(mod.exog,columns=mod.exog_names)
print(mod_matrix)
```

```
   Intercept   x1   x2
0        1.0  7.4  1.0
1        1.0  1.2  1.0
2        1.0  3.1  2.0
3        1.0  4.8  2.0
4        1.0  2.8  3.0
5        1.0  6.5  3.0
```

Suppose the second variable is actually qualitative; e.g., it represents a color, and the levels 1, 2, and 3 stand for red, blue, and green. We can account for such a categorical variable by using the **astype** method to redefine the data type (see Section 1.2).

☞ 3

```
myData['x2'] = myData['x2'].astype('category')
```

Alternatively, a categorical variable can be specified in the model formula by wrapping it with `C()`. Observe how this changes the model matrix.

```
mod2 = ols("y~x1+C(x2)", data=myData)
mod2_matrix = pd.DataFrame(mod2.exog,columns=mod2.exog_names)
print(mod2_matrix)
```

```
   Intercept  C(x2)[T.2]  C(x2)[T.3]   x1
0        1.0         0.0         0.0  7.4
1        1.0         0.0         0.0  1.2
2        1.0         1.0         0.0  3.1
3        1.0         1.0         0.0  4.8
4        1.0         0.0         1.0  2.8
5        1.0         0.0         1.0  6.5
```

Thus, if a **statsmodels** formula of the form (5.32) contains factor (qualitative) variables, the model is no longer of the form (5.33), but contains indicator variables for each level of the factor variable, except the first level.

For the case above, the corresponding linear model is

$$Y_i = \beta_0 + \beta_1 x_{i1} + \alpha_2 \mathbb{1}\{x_{i2} = 2\} + \alpha_3 \mathbb{1}\{x_{i2} = 3\} + \varepsilon_i, \quad i = 1, \ldots, 6, \tag{5.34}$$

where we have used parameters α_2 and α_3 to correspond to the indicator features of the qualitative variable. The parameter α_2 describes how much the response is expected to

change if the factor x_2 switches from level 1 to 2. A similar interpretation holds for α_3. Such parameters can thus be viewed as incremental effects.

It is also possible to model *interaction* between two variables. For two continuous variables, this simply adds the products of the original features to the model matrix. Adding interaction terms in Python is achieved by replacing "+" in the formula with "*", as the following example illustrates. INTERACTION

```
mod3 = ols("y~x1*C(x2)", data=myData)
mod3_matrix = pd.DataFrame(mod3.exog,columns=mod3.exog_names)
print(mod3_matrix)
```

```
   Intercept  C(x2)[T.2]  C(x2)[T.3]   x1  x1:C(x2)[T.2]  x1:C(x2)[T.3]
0        1.0         0.0         0.0  7.4            0.0            0.0
1        1.0         0.0         0.0  1.2            0.0            0.0
2        1.0         1.0         0.0  3.1            3.1            0.0
3        1.0         1.0         0.0  4.8            4.8            0.0
4        1.0         0.0         1.0  2.8            0.0            2.8
5        1.0         0.0         1.0  6.5            0.0            6.5
```

5.6.2 Analysis

Let us consider some easy linear regression models by using the student survey data set `survey.csv` from the book's GitHub site, which contains measurements such as height, weight, sex, etc., from a survey conducted among $n = 100$ university students. Suppose we wish to investigate the relation between the shoe size (explanatory variable) and the height (response variable) of a person. First, we load the data and draw a scatterplot of the points (height versus shoe size); see Figure 5.6 (without the fitted line).

```
survey = pd.read_csv('survey.csv')
plt.scatter(survey.shoe, survey.height)
plt.xlabel("Shoe size")
plt.ylabel("Height")
```

We observe a slight increase in the height as the shoe size increases, although this relationship is not very distinct. We analyze the data through the simple linear regression model $Y_i = \beta_0 + \beta_1 x_i + \varepsilon_i, i = 1, \ldots, n$. In **statsmodels** this is performed via the **ols** method as follows: ☞ 169

```
model = ols("height~shoe", data=survey) # define the model
fit = model.fit()  #fit the model defined above
b0, b1 = fit.params
print(fit.params)
```

```
Intercept    145.777570
shoe           1.004803
dtype: float64
```

The above output gives the least-squares estimates of β_0 and β_1. For this example, we have $\widehat{\beta}_0 = 145.778$ and $\widehat{\beta}_1 = 1.005$. Figure 5.6, which includes the regression line, was obtained as follows:

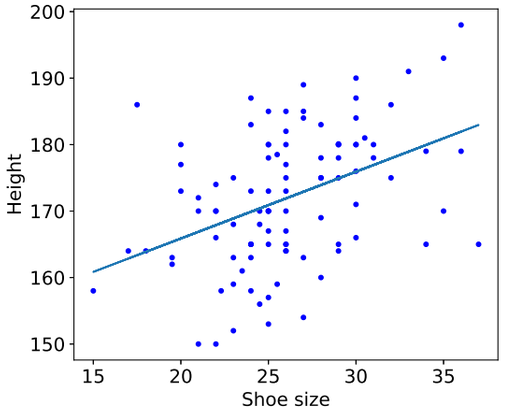


Figure 5.6: Scatterplot of height (cm) against shoe size (cm), with the fitted line.

```
plt.plot(survey.shoe, b0 + b1*survey.shoe)
plt.scatter(survey.shoe, survey.height)
plt.xlabel("Shoe size")
plt.ylabel("Height")
```

Although `ols` performs a complete analysis of the linear model, not all its calculations need to be presented. A summary of the results can be obtained with the method `summary`.

```
print(fit.summary())
```

```
Dep. Variable:            height   R-squared:                       0.178
Model:                       OLS   Adj. R-squared:                  0.170
Method:            Least Squares   F-statistic:                     21.28
No. Observations:             100   Prob (F-statistic):           1.20e-05
Df Residuals:                  98   Log-Likelihood:                -363.88
Df Model:                       1   AIC:                             731.8
Covariance Type:        nonrobust   BIC:                             737.0
==============================================================================
                 coef    std err          t      P>|t|      [0.025      0.975]
------------------------------------------------------------------------------
Intercept    145.7776      5.763     25.296      0.000     134.341     157.214
shoe           1.0048      0.218      4.613      0.000       0.573       1.437
==============================================================================
Omnibus:                        1.958   Durbin-Watson:                   1.772
Prob(Omnibus):                  0.376   Jarque-Bera (JB):                1.459
Skew:                          -0.072   Prob(JB):                        0.482
Kurtosis:                       2.426   Cond. No.                         164.
```

The main output items are the following:

- `coef:` Estimates of the parameters of the regression line.
- `std error:` Standard deviations of the estimators of the regression line. These are the square roots of the variances of the $\{\widehat{\beta}_i\}$ obtained in (5.25).

☞ 186

- `t:` Realization of Student's test statistics associated with the hypotheses $H_0 : \beta_i = 0$ and $H_1 : \beta_i \neq 0$, $i = 0, 1$. In particular, the outcome of T in (5.19). ☞ 183
- `P>|t|`: P-value of Student's test (two-sided test).
- `[0.025 0.975]`: 95% confidence intervals for the parameters.
- `R-Squared:` Coefficient of determination R^2 (percentage of variation explained by the regression), as defined in (5.18). ☞ 181
- `Adj. R-Squared:` adjusted R^2 (explained in Section 5.3.7).
- `F-statistic:` Realization of the F test statistic (5.21) associated with testing the full model against the default model. The associated degrees of freedom (`Df Model` = 1 and `Df Residuals` = $n-2$) are given, as is the P-value: `Prob (F-statistic)`. ☞ 183
- `AIC:` The AIC number in (5.15); that is, minus two times the log-likelihood plus two times the number of model parameters (which is 3 here). ☞ 177

You can access all the numerical values as they are attributes of the `fit` object. First check which names are available, as in:

```
dir(fit)
```

Then access the values via the dot construction. For example, the following extracts the P-value for the slope.

```
fit.pvalues[1]
```

```
1.1994e-05
```

The results show strong evidence for a linear relationship between shoe size and height (or, more accurately, strong evidence that the slope of the regression line is not zero), as the P-value for the corresponding test is very small ($1.2 \cdot 10^{-5}$). The estimate of the slope indicates that the difference between the average height of students whose shoe size is different by one cm is 1.0048 cm.

Only 17.84% of the variability of student height is explained by the shoe size. We therefore need to add other explanatory variables to the model (multiple linear regression) to increase the model's predictive power.

5.6.3 Analysis of Variance (ANOVA)

We continue the student survey example of the previous section, but now add an extra variable, and also consider an analysis of variance of the model. Instead of "explaining" the student height via their shoe size, we include `weight` as an explanatory variable. The corresponding `ols` formula for this model is

$$\texttt{height} \sim \texttt{shoe} + \texttt{weight},$$

meaning that each random height, denoted by `Height`, satisfies

$$\texttt{Height} = \beta_0 + \beta_1 \texttt{shoe} + \beta_2 \texttt{weight} + \varepsilon,$$

where ε is a normally distributed error term with mean 0 and variance σ^2. Thus, the model has 4 parameters. Before analyzing the model we present a scatterplot of all pairs of variables, using `scatter_matrix`.

```
model = ols("height~shoe+weight", data=survey)
fit = model.fit()
axes = pd.plotting.scatter_matrix(
            survey[['height','shoe','weight']])
plt.show()
```

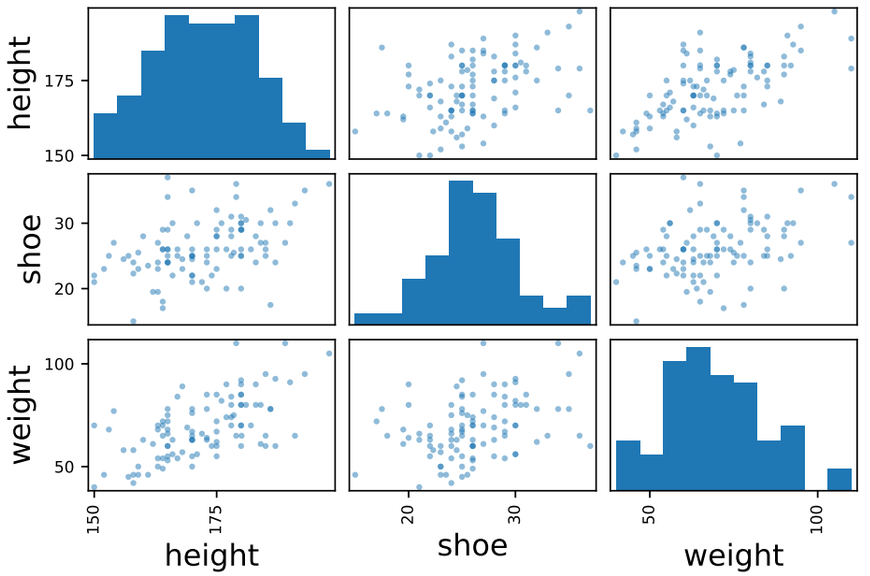


Figure 5.7: Scatterplot of all pairs of variables: height (cm), shoe (cm), and weight (kg).

As for the simple linear regression model in the previous section, we can analyze the model using the `summary` method (below we have omitted some output):

```
fit.summary()
```

```
Dep. Variable:              height   R-squared:                      0.430
Model:                         OLS   Adj. R-squared:                 0.418
Method:              Least Squares   F-statistic:                    36.61
No. Observations:              100   Prob (F-statistic):          1.43e-12
Df Residuals:                   97   Log-Likelihood:                -345.58
Df Model:                        2   AIC:                             697.2
                                     BIC:                             705.0
==============================================================================
                 coef    std err          t      P>|t|      [0.025      0.975]
------------------------------------------------------------------------------
Intercept    132.2677      5.247     25.207      0.000     121.853     142.682
```

```
shoe          0.5304     0.196     2.703     0.008     0.141     0.920
weight        0.3744     0.057     6.546     0.000     0.261     0.488
```

The `F-statistic` is used to test whether the full model (here with two explanatory variables) is better at "explaining" the height than the default model. The corresponding null hypothesis is $H_0 : \beta_1 = \beta_2 = 0$. The assertion of interest is H_1: at least one of the coefficients β_j ($j = 1, 2$) is significantly different from zero. Given the result of this test (P-value $= 1.429 \cdot 10^{-12}$), we can conclude that at least one of the explanatory variables is associated with height. The individual Student tests indicate that:

- shoe size is linearly associated with student height, after adjusting for weight, with P-value 0.0081. At the same weight, an increase of one cm in shoe size corresponds to an increase of 0.53 cm in average student height;
- weight is linearly associated with student height, after adjusting for shoe size (the P-value is actually $2.82 \cdot 10^{-09}$; the reported value of 0.000 should be read as "less than 0.001"). At the same shoe size, an increase of one kg in weight corresponds to an increase of 0.3744 cm in average student height.

Further understanding is extracted from the model by conducting an analysis of variance. The standard **statsmodels** function is **anova_lm**. The input to this function is the fit object (obtained from `model.fit()`) and the output is a `DataFrame` object.

```
table = sm.stats.anova_lm(fit)
print(table)
```

```
              df   sum_sq        mean_sq        F          PR(>F)
shoe         1.0  1840.467359  1840.467359  30.371310  2.938651e-07
weight       1.0  2596.275747  2596.275747  42.843626  2.816065e-09
Residual    97.0  5878.091294    60.598879        NaN           NaN
```

The meaning of the columns is as follows.

- `df` : The degrees of freedom of the variables, according to the sum of squares decomposition (5.17). As both `shoe` and `weight` are quantitative variables, their degrees of freedom are both 1 (each corresponding to a single column in the overall model matrix). The degrees of freedom for the residuals is $n - p = 100 - 3 = 97$. ☞ 181
- `sum_sq`: The sum of squares according to (5.17). The total sum of squares is the sum of all the entries in this column. The residual error in the model that cannot be explained by the variables is RSS ≈ 5878.
- `mean_sq`: The sum of squares divided by their degrees of freedom. Note that the residual square error RSE $=$ RSS$/(n - p) = 60.6$ is an unbiased estimate of the model variance σ^2; see Section 5.4. ☞ 182
- `F`: These are the outcomes of the test statistic (5.22). ☞ 184
- `PR(>F)`: These are the P-values corresponding to the test statistic in the preceding column and are computed using an `F` distribution whose degrees of freedom are given in the `df` column.

The ANOVA table indicates that the `shoe` variable explains a reasonable amount of the variation in the model, as evidenced by a sum of squares contribution of 1840 out of 1840+2596+5878 = 10314 and a very small P-value. After `shoe` is included in the model, it turns out that the `weight` variable explains even more of the remaining variability, with an even smaller P-value. The remaining sum of squares (5878) is 57% of the total sum of squares, yielding a 43% reduction, in accordance with the R^2 value reported in the summary for the `ols` method. As mentioned in Section 5.4.1, the *order* in which the ANOVA is conducted is important. To illustrate this, consider the output of the following commands.

```
model = ols("height~weight+shoe", data=survey)
fit = model.fit()
table = sm.stats.anova_lm(fit)
print(table)
```

```
            df    sum_sq       mean_sq       F           PR(>F)
weight     1.0  3993.860167  3993.860167  65.906502  1.503553e-12
shoe       1.0   442.882938   442.882938   7.308434  8.104688e-03
Residual  97.0  5878.091294    60.598879        NaN           NaN
```

We see that `weight` as a single model variable explains much more of the variability than `shoe` did. If we now also include `shoe`, we only obtain a small (but according to the P-value still significant) reduction in the model variability.

5.6.4 Confidence and Prediction Intervals

In `statsmodels` a method for computing confidence or prediction intervals from a dictionary of explanatory variables is `get_prediction`. It simply executes formula (5.24) or (5.26). A simpler version is `predict`, which only returns the predicted value.

☞ 186

Continuing the student survey example, suppose we wish to predict the height of a person with shoe size 30 cm and weight 75 kg. Confidence and prediction intervals can be obtained as given in the code below. The new explanatory variable is entered as a dictionary. Notice that the 95% prediction interval (for the corresponding random response) is much wider than the 95% confidence interval (for the expectation of the random response).

```
x = {'shoe': [30.0], 'weight': [75.0]}  # new input (dictionary)
pred = fit.get_prediction(x)
pred.summary_frame(alpha=0.05).unstack()
```

```
mean            0    176.261722    # predicted value
mean_se         0      1.054015
mean_ci_lower   0    174.169795    # lower bound for CI
mean_ci_upper   0    178.353650    # upper bound for CI
obs_ci_lower    0    160.670610    # lower bound for PI
obs_ci_upper    0    191.852835    # upper bound for PI
dtype: float64
```

5.6.5 Model Validation

We can perform an analysis of residuals to examine whether the underlying assumptions of the (normal) linear regression model are verified. Various plots of the residuals can be

used to inspect whether the assumptions on the errors $\{\varepsilon_i\}$ are satisfied. Figure 5.8 gives two such plots. The first is a scatterplot of the residuals $\{e_i\}$ against the fitted values $\widehat{y_i}$. When the model assumptions are valid, the residuals, as approximations of the model error, should behave approximately as iid normal random variables for each of the fitted values, with a constant variance. In this case we see no strong aberrant structure in this plot. The residuals are fairly evenly spread and symmetrical about the $y = 0$ line (not shown). The second plot is a quantile–quantile (or qq) plot. This is a useful way to check for normality of the error terms, by plotting the sample quantiles of the residuals against the theoretical quantiles of the standard normal distribution. Under the model assumptions, the points should lie approximately on a straight line. For the current case there does not seem to be an extreme departure from normality. Drawing a histogram or density plot of the residuals will also help to verify the normality assumption. The following code was used.

```
plt.plot(fit.fittedvalues,fit.resid,'.')
plt.xlabel("fitted values")
plt.ylabel("residuals")
sm.qqplot(fit.resid)
```

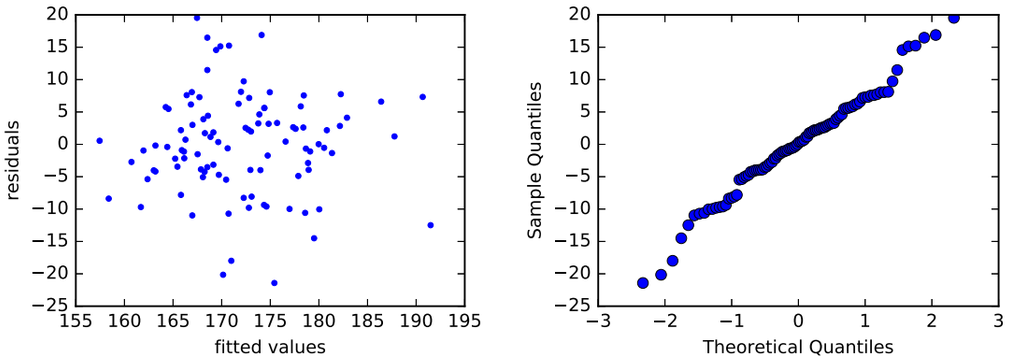


Figure 5.8: Left: residuals against fitted values. Right: a qq plot of the residuals. Neither shows clear evidence against the model assumptions of constant variance and normality.

5.6.6 Variable Selection

Among the large number of possible explanatory variables, we wish to select those which best explain the observed responses. By eliminating redundant explanatory variables, we reduce the statistical error without increasing the approximation error, and thus reduce the (expected) generalization risk of the learner.

In this section, we briefly present two methods for variable selection. They are illustrated on a few variables from the data set **birthwt** discussed in Section 1.5.3.2. The data set contains information on the birth weights (masses) of babies, as well as various characteristics of the mother, such as whether she smokes, her age, etc. We wish to explain the child's weight at birth using various characteristics of the mother, her family history, and her behavior during pregnancy. The response variable is weight at birth (quantitative variable `bwt`, expressed in grams); the explanatory variables are given below.

☞ 13

The data can be obtained as explained in Section 1.5.3.2, or from `statsmodels` in the following way:

```
bwt = sm.datasets.get_rdataset("birthwt","MASS").data
```

Here is some information about the explanatory variables that we will investigate.

```
age:   mother's age in years
lwt:   mother's weight in lbs
race:  mother's race (1 = white, 2 = black, 3 = other)
smoke: smoking status during pregnancy (0 = no, 1 = yes)
ptl:   no. of previous premature labors
ht:    history of hypertension (0 = no, 1 = yes)
ui:    presence of uterine irritability (0 = no, 1 = yes)
ftv:   no. of physician visits during first trimester
bwt:   birth weight in grams
```

We can see the structure of the variables via `bwt.info()`. Check yourself that all variables are defined as *quantitative* (`int64`). However, the variables `race`, `smoke`, `ht`, and `ui` should really be interpreted as *qualitative* (factors). To fix this, we could redefine them with the method `astype`, similar to what we did in Chapter 1. Alternatively, we could use the `C()` construction in a `statsmodels` formula to let the program know that certain variables are factors. We will use the latter approach.

For *binary* features it does not matter whether the variables are interpreted as factorial or numerical as the numerical and summary results are identical.

We consider the explanatory variables `lwt`, `age`, `ui`, `smoke`, `ht`, and two recoded binary variables `ftv1` and `ptl1`. We define `ftv1` = 1 if there was at least one visit to a physician, and `ftv1` = 0 otherwise. Similarly, we define `ptl1` = 1 if there is at least one preterm birth in the family history, and `ptl1` = 0 otherwise.

```
ftv1 = (bwt['ftv']>=1).astype(int)
ptl1 = (bwt['ptl']>=1).astype(int)
```

5.6.6.1 Forward Selection and Backward Elimination

FORWARD SELECTION

The *forward selection* method is an iterative method for variable selection. In the first iteration we consider which feature `f1` is the most significant in terms of its P-value in the models `bwt~f1`, with `f1` $\in$ {`lwt`, `age`, ...}. This feature is then selected into the model. In the second iteration, the feature `f2` that has the smallest P-value in the models `bwt~f1+f2` is selected, where `f2` $\neq$ `f1`, and so on. Usually only features are selected that have a P-value of at most 0.05. The following Python program automates this procedure. Instead of selecting on the P-value one could select on the AIC or BIC value.

forwardselection.py

```
import statsmodels.api as sm
from statsmodels.formula.api import ols

bwt = sm.datasets.get_rdataset("birthwt","MASS").data
ftv1 = (bwt['ftv']>=1).astype(int)
ptl1 = (bwt['ptl']>=1).astype(int)

remaining_features = {'lwt', 'age', 'C(ui)', 'smoke',
                      'C(ht)', 'ftv1', 'ptl1'}
selected_features = []
while remaining_features:
  PF = []  #list of (P value, feature)
  for f in remaining_features:
    temp = selected_features + [f]  #temporary list of features
    formula = 'bwt~' + '+'.join(temp)
    fit = ols(formula,data=bwt).fit()
    pval= fit.pvalues[-1]
    if pval < 0.05:
       PF.append((pval,f))
  if PF:  #if not empty
     PF.sort(reverse=True)
     (best_pval, best_f) = PF.pop()
     remaining_features.remove(best_f)
     print('feature {} with P-value = {:.2E}'.
           format(best_f, best_pval))
     selected_features.append(best_f)
  else:
     break
```

```
feature C(ui) with P-value = 7.52E-05
feature C(ht) with P-value = 1.08E-02
feature lwt with P-value = 6.01E-03
feature smoke with P-value = 7.27E-03
```

BACKWARD ELIMINATION

In *backward elimination* we start with the complete model (all features included) and at each step, we remove the variable with the highest P-value, as long as it is not significant (greater than 0.05). We leave it as an exercise to verify that the order in which the features are removed is: `age`, `ftv1`, and `ptl1`. In this case, forward selection and backward elimination result in the same model, but this need not be the case in general.

This way of model selection has the advantage of being easy to use and of treating the question of variable selection in a systematic manner. The main drawback is that variables are included or deleted based on purely statistical criteria, without taking into account the aim of the study. This usually leads to a model which may be satisfactory from a statistical point of view, but in which the variables are not necessarily the most relevant when it comes to understanding and interpreting the data in the study.

Of course, we can choose to investigate any combination of features, not just the ones suggested by the above variable selection methods. For example, let us see if the mother's weight, her age, her race, and whether she smokes explain the baby's birthweight.

```
formula = 'bwt~lwt+age+C(race)+ smoke'
bwt_model = ols(formula, data=bwt).fit()
print(bwt_model.summary())
```

```
                            OLS Regression Results
==============================================================================
Dep. Variable: bwt             R-squared: 0.148
Model: OLS                     Adj. R-squared: 0.125
Method: Least Squares          F-statistic: 6.373
No. Observations: 189          Prob (F-statistic):  1.76e-05
Df Residuals: 183              Log-Likelihood: -1498.4
Df Model: 5                    AIC: 3009.
                               BIC: 3028.
==============================================================================
                   coef    std err      t      P>|t|  [0.025      0.975]
------------------------------------------------------------------------------
Intercept     2839.4334   321.435    8.834   0.000  2205.239    3473.628
C(race)[T.2]  -510.5015   157.077   -3.250   0.001  -820.416    -200.587
C(race)[T.3]  -398.6439   119.579   -3.334   0.001  -634.575    -162.713
smoke         -401.7205   109.241   -3.677   0.000  -617.254    -186.187
lwt              3.9999     1.738    2.301   0.022     0.571       7.429
age             -1.9478     9.820   -0.198   0.843   -21.323      17.427
==============================================================================
Omnibus: 3.916                 Durbin-Watson: 0.458
Prob(Omnibus): 0.141           Jarque-Bera (JB): 3.718
Skew: -0.343                   Prob(JB): 0.156
Kurtosis: 3.038                Cond. No. 899.
```

Given the result of Fisher's global test given by `Prob (F-Statistic)` in the summary (P-value = 1.76×10^{-5}), we can conclude that at least one of the explanatory variables is associated with child weight at birth, after adjusting for the other variables. The individual Student tests indicate that:

- the mother's weight is linearly associated with child weight, after adjusting for age, race, and smoking status (P-value = 0.022). At the same age, race, and smoking status, an increase of one pound in the mother's weight corresponds to an increase of 4 g in the average child weight at birth;

- the age of the mother is not significantly linearly associated with child weight at birth, when mother weight, race, and smoking status are already taken into account (P-value = 0.843);

- weight at birth is significantly lower for a child born to a mother who smokes, compared to children born to non-smoking mothers of the same age, race, and weight, with a P-value of 0.00031 (to see this, inspect `bwt_model.pvalues`). At the same age, race, and mother weight, the child's weight at birth is 401.720 g less for a smoking mother than for a non-smoking mother;

- regarding the interpretation of the variable `race`, we note that the first level of this categorical variable corresponds to white mothers. The estimate of −510.501 g for `C(race)[T.2]` represents the difference in the child's birth weight between black mothers and white mothers (reference group), and this result is significantly different

from zero (P-value = 0.001) in a model adjusted for the mother's weight, age, and smoking status.

5.6.6.2 Interaction

We can also include interaction terms in the model. Let us see whether there is any interaction effect between `smoke` and `age` via the model

$$\texttt{Bwt} = \beta_0 + \beta_1 \texttt{age} + \beta_2 \texttt{smoke} + \beta_3 \texttt{age} \times \texttt{smoke} + \varepsilon.$$

In `Python` this can be done as follows (below we have removed some output):

```
formula = 'bwt~age*smoke'
bwt_model = ols(formula, data=bwt).fit()
print(bwt_model.summary())
```

```
                            OLS Regression Results
==============================================================================
Dep. Variable: bwt         R-squared: 0.069
Model: OLS                 Adj. R-squared: 0.054
Method: Least Squares      F-statistic: 4.577
No. Observations: 189      Prob (F-statistic):  0.00407
Df Residuals: 183          Log-Likelihood: -1506.8
Df Model: 5                AIC: 3009.
                           BIC: 3028.
==============================================================================
                 coef    std err     t      P>|t|    [0.025    0.975]
------------------------------------------------------------------------------
Intercept      2406.1   292.190    8.235    0.000   1829.6    2982.5
smoke           798.2   484.342    1.648    0.101   -157.4    1753.7
age              27.7    12.149    2.283    0.024      3.8      51.7
age:smoke       -46.6    20.447   -2.278    0.024    -86.9      -6.2
```

We observe that the estimate for β_3 (-46.6) is significantly different from zero (P-value = 0.024). We therefore conclude that the effect of the mother's age on the child's weight depends on the smoking status of the mother. The results on association between mother age and child weight must therefore be presented separately for the smoking and the non-smoking group. For non-smoking mothers (`smoke = 0`), the mean child weight at birth increases on average by 27.7 grams for each year of the mother's age. This is statistically significant, as can be seen from the 95% confidence intervals for the parameters (which does not contain zero):

```
bwt_model.conf_int()
```

```
                     0            1
Intercept  1829.605754  2982.510194
age           3.762780    51.699977
smoke      -157.368023  1753.717779
age:smoke   -86.911405    -6.232425
```

Similarly, for smoking mothers, there seems to be a decrease in birthweight, $\widehat{\beta_1} + \widehat{\beta_3} = 27.7 - 46.6 = -18.9$, but this is not statistically significant; see Exercise 6.

5.7 Generalized Linear Models

The normal linear model in Section 2.8 deals with continuous response variables — such as height and crop yield — and continuous or discrete explanatory variables. Given the feature vectors $\{\boldsymbol{x}_i\}$, the responses $\{Y_i\}$ are independent of each other, and each has a normal distribution with mean $\boldsymbol{x}_i^\top \boldsymbol{\beta}$, where $\boldsymbol{x}_i^\top$ is the i-th row of the model matrix $\mathbf{X}$. Generalized linear models allow for arbitrary response distributions, including *discrete* ones.

Definition 5.2: Generalized Linear Model

GENERALIZED LINEAR MODEL

In a *generalized linear model* (GLM) the expected response for a given feature vector $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$ is of the form

$$\mathbb{E}[Y \,|\, \mathbf{X} = \boldsymbol{x}] = h(\boldsymbol{x}^\top \boldsymbol{\beta}) \tag{5.35}$$

ACTIVATION FUNCTION

for some function h, which is called the *activation function*. The distribution of Y (for a given $\boldsymbol{x}$) may depend on additional *dispersion* parameters that model the randomness in the data that is not explained by $\boldsymbol{x}$.

LINK FUNCTION

The *inverse* of function h is called the *link function*. As for the linear model, (5.35) is a model for a single pair $(\boldsymbol{x}, Y)$. Using the model simplification introduced at the end of Section 5.1, the corresponding model for a whole training set $\mathcal{T} = \{(\boldsymbol{x}_i, Y_i)\}$ is that the $\{\boldsymbol{x}_i\}$ are fixed and that the $\{Y_i\}$ are independent; each Y_i satisfying (5.35) with $\boldsymbol{x} = \boldsymbol{x}_i$. Writing $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$ and defining $\boldsymbol{h}$ as the multivalued function with components h, we have

$$\mathbb{E}_{\mathbf{X}} \boldsymbol{Y} = \boldsymbol{h}(\mathbf{X}\boldsymbol{\beta}),$$

where $\mathbf{X}$ is the (model) matrix with rows $\boldsymbol{x}_1^\top, \ldots, \boldsymbol{x}_n^\top$. A common assumption is that $Y_1, \ldots, Y_n$ come from the same family of distributions, e.g., normal, Bernoulli, or Poisson. The central focus is the parameter vector $\boldsymbol{\beta}$, which summarizes how the matrix of explanatory variables $\mathbf{X}$ affects the response vector $\boldsymbol{Y}$. The class of generalized linear models can encompass a wide variety of models. Obviously the normal linear model (2.34) is a generalized linear model, with $\mathbb{E}[Y \,|\, \mathbf{X} = \boldsymbol{x}] = \boldsymbol{x}^\top \boldsymbol{\beta}$, so that h is the identity function. In this case, $Y \sim \mathcal{N}(\boldsymbol{x}^\top \boldsymbol{\beta}, \sigma^2)$, $i = 1, \ldots, n$, where σ^2 is a dispersion parameter.

LOGISTIC REGRESSION

LOGISTIC DISTRIBUTION

■ **Example 5.10 (Logistic Regression)** In a *logistic regression* or *logit model*, we assume that the response variables $Y_1, \ldots, Y_n$ are independent and distributed according to $Y_i \sim \mathsf{Ber}(h(\boldsymbol{x}_i^\top \boldsymbol{\beta}))$, where h here is defined as the cdf of the *logistic distribution*:

$$h(x) = \frac{1}{1 + \mathrm{e}^{-x}}.$$

Large values of $\boldsymbol{x}_i^\top \boldsymbol{\beta}$ thus lead to a high probability that $Y_i = 1$, and small (negative) values of $\boldsymbol{x}_i^\top \boldsymbol{\beta}$ cause Y_i to be 0 with high probability. Estimation of the parameter vector $\boldsymbol{\beta}$ from the observed data is not as straightforward as for the ordinary linear model, but can be accomplished via the minimization of a suitable training loss, as explained below.

As the $\{Y_i\}$ are independent, the pdf of $\boldsymbol{Y} = [Y_1, \ldots, Y_n]^\top$ is

$$g(\boldsymbol{y} \,|\, \boldsymbol{\beta}, \mathbf{X}) = \prod_{i=1}^{n} [h(\boldsymbol{x}_i^\top \boldsymbol{\beta})]^{y_i} [1 - h(\boldsymbol{x}_i^\top \boldsymbol{\beta})]^{1-y_i}.$$

Maximizing the log-likelihood $\ln g(\boldsymbol{y} \,|\, \boldsymbol{\beta}, \mathbf{X})$ with respect to $\boldsymbol{\beta}$ gives the maximum likelihood estimator of $\boldsymbol{\beta}$. In a supervised learning framework, this is equivalent to minimizing:

$$\begin{aligned} -\frac{1}{n} \ln g(\boldsymbol{y} \,|\, \boldsymbol{\beta}, \mathbf{X}) &= -\frac{1}{n} \sum_{i=1}^{n} \ln g(y_i \,|\, \boldsymbol{\beta}, \boldsymbol{x}_i) \\ &= -\frac{1}{n} \sum_{i=1}^{n} \left[y_i \ln h(\boldsymbol{x}_i^\top \boldsymbol{\beta}) + (1 - y_i) \ln(1 - h(\boldsymbol{x}_i^\top \boldsymbol{\beta})) \right]. \end{aligned} \tag{5.36}$$

By comparing (5.36) with (4.4), we see that we can interpret (5.36) as the *cross-entropy training loss* associated with comparing a true conditional pdf $f(y \,|\, \boldsymbol{x})$ with an approximation pdf $g(y \,|\, \boldsymbol{\beta}, \boldsymbol{x})$ via the loss function ☞ 123

$$\text{Loss}(f(y \,|\, \boldsymbol{x}), g(y \,|\, \boldsymbol{\beta}, \boldsymbol{x})) := -\ln g(y \,|\, \boldsymbol{\beta}, \boldsymbol{x}) = -y \ln h(\boldsymbol{x}^\top \boldsymbol{\beta}) - (1 - y) \ln(1 - h(\boldsymbol{x}^\top \boldsymbol{\beta})).$$

Minimizing (5.36) in terms of $\boldsymbol{\beta}$ actually constitutes a *convex* optimization problem. Since $\ln h(\boldsymbol{x}^\top \boldsymbol{\beta}) = -\ln(1 + \mathrm{e}^{-\boldsymbol{x}^\top \boldsymbol{\beta}})$ and $\ln(1 - h(\boldsymbol{x}^\top \boldsymbol{\beta})) = -\boldsymbol{x}^\top \boldsymbol{\beta} - \ln(1 + \mathrm{e}^{-\boldsymbol{x}^\top \boldsymbol{\beta}})$, the cross-entropy training loss (5.36) can be rewritten as

$$r_\tau(\boldsymbol{\beta}) := \frac{1}{n} \sum_{i=1}^{n} \left[(1 - y_i) \boldsymbol{x}_i^\top \boldsymbol{\beta} + \ln\left(1 + \mathrm{e}^{-\boldsymbol{x}_i^\top \boldsymbol{\beta}}\right) \right].$$

We leave it as Exercise 7 to show that the gradient $\nabla r_\tau(\boldsymbol{\beta})$ and Hessian $\mathbf{H}(\boldsymbol{\beta})$ of $r_\tau(\boldsymbol{\beta})$ are given by

$$\nabla\, r_\tau(\boldsymbol{\beta}) = \frac{1}{n} \sum_{i=1}^{n} (\mu_i - y_i)\, \boldsymbol{x}_i \tag{5.37}$$

and

$$\mathbf{H}(\boldsymbol{\beta}) = \frac{1}{n} \sum_{i=1}^{n} \mu_i (1 - \mu_i)\, \boldsymbol{x}_i\, \boldsymbol{x}_i^\top, \tag{5.38}$$

respectively, where $\mu_i := h(\boldsymbol{x}_i^\top \boldsymbol{\beta})$.

Notice that $\mathbf{H}(\boldsymbol{\beta})$ is a positive semidefinite matrix for all values of $\boldsymbol{\beta}$, implying the convexity of $r_\tau(\boldsymbol{\beta})$. Consequently, we can find an optimal $\boldsymbol{\beta}$ efficiently; e.g., via Newton's method. Specifically, given an initial value $\boldsymbol{\beta}_0$, for $t = 1, 2, \ldots$, iteratively compute ☞ 405 ☞ 411

$$\boldsymbol{\beta}_t = \boldsymbol{\beta}_{t-1} - \mathbf{H}^{-1}(\boldsymbol{\beta}_{t-1})\, \nabla r_\tau(\boldsymbol{\beta}_{t-1}), \tag{5.39}$$

until the sequence $\boldsymbol{\beta}_0, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots$ is deemed to have converged, using some pre-fixed convergence criterion.

Figure 5.9 shows the outcomes of 100 independent Bernoulli random variables, where each success probability, $(1 + \exp(-(\beta_0 + \beta_1 x)))^{-1}$, depends on x and $\beta_0 = -3$, $\beta_1 = 10$. The true logistic curve is also shown (dashed line). The minimum training loss curve (red line) is obtained via the Newton scheme (5.39), giving estimates $\widehat{\beta_0} = -2.66$ and $\widehat{\beta_1} = 10.08$. The Python code is given below.

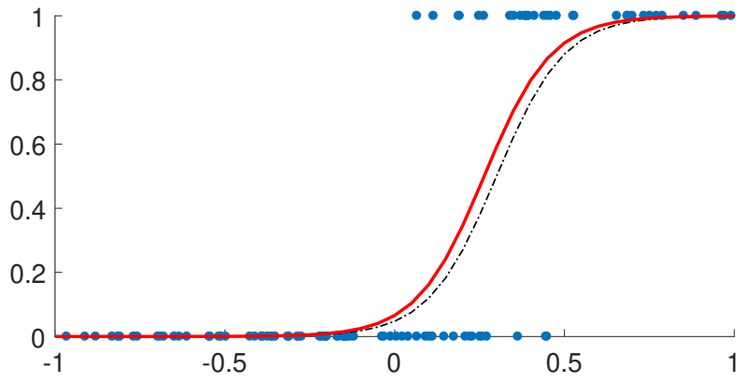


Figure 5.9: Logistic regression data (blue dots), fitted curve (red), and true curve (black dashed).

logreg1d.py

```
import numpy as np
import matplotlib.pyplot as plt
from  numpy.linalg import lstsq

n = 100                                          # sample size
x = (2*np.random.rand(n)-1).reshape(n,1)  # explanatory variables
beta = np.array([-3, 10])
Xmat = np.hstack((np.ones((n,1)), x))
p = 1/(1 + np.exp(-Xmat @ beta))
y = np.random.binomial(1,p,n)                # response variables

# initial guess
betat = lstsq((Xmat.T @ Xmat),Xmat.T @ y, rcond=None)[0]

grad = np.array([2,1])                                  # gradient

while (np.sum(np.abs(grad)) > 1e-5) :      # stopping criteria
    mu = 1/(1+np.exp(-Xmat @ betat))
    # gradient
    delta = (mu - y).reshape(n,1)
    grad = np.sum(np.multiply( np.hstack((delta,delta)),Xmat), axis
        =0).T
    # Hessian
    H = Xmat.T @ np.diag(np.multiply(mu,(1-mu))) @ Xmat
    betat = betat - lstsq(H,grad,rcond=None)[0]
    print(betat)

plt.plot(x,y, '.') # plot data

xx = np.linspace(-1,1,40).reshape(40,1)
XXmat = np.hstack( (np.ones((len(xx),1)), xx))
yy = 1/(1 + np.exp(-XXmat @ beta))
plt.plot(xx,yy,'r-')                        #true logistic curve
yy = 1/(1 + np.exp(-XXmat @ betat));
plt.plot(xx,yy,'k--')
```

Further Reading

An excellent overview of regression is provided in [33] and an accessible mathematical treatment of *linear* regression models can be found in [108]. For extensions to *nonlinear* regression we refer the reader to [7]. A practical introduction to multilevel/hierarchical models is given in [47]. For further discussion on regression with discrete responses (classification) we refer to Chapter 7 and the further reading therein. On the important question of how to handle missing data, the classic reference is [80] (see also [85]) and a modern applied reference is [120].

☞ 253

Exercises

1. Following his mentor Francis Galton, the mathematician/statistician Karl Pearson conducted comprehensive studies comparing hereditary traits between members of the same family. Figure 5.10 depicts the measurements of the heights of 1078 fathers and their adult sons (one son per father). The data is available from the book's GitHub site as `pearson.csv`.

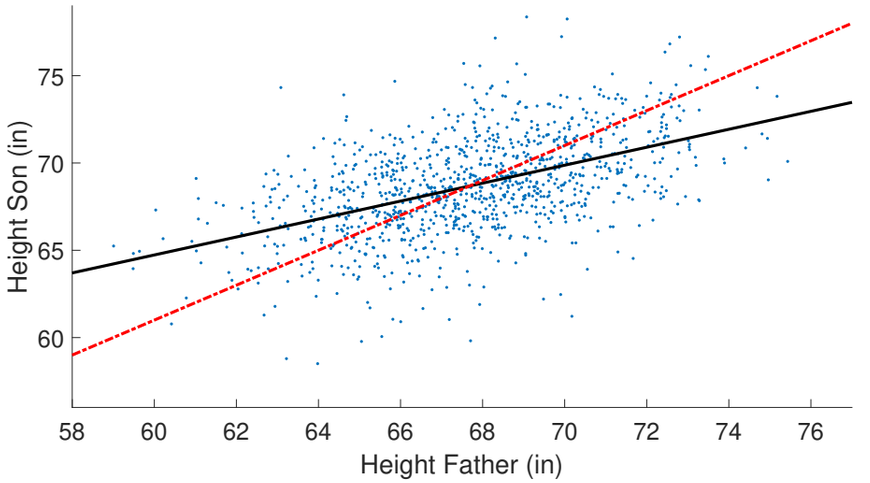


Figure 5.10: A scatterplot of heights from Pearson's data.

(a) Show that sons are on average 1 inch taller than the fathers.

(b) We could try to "explain" the height of the son by taking the height of his father and adding 1 inch. The prediction line $y = x + 1$ (red dashed) is given Figure 5.10. The black solid line is the fitted regression line. This line has a slope less than 1, and demonstrates Galton's "regression" to the average. Find the intercept and slope of the fitted regression line.

2. For the simple linear regression model, show that the values for $\widehat{\beta}_1$ and $\widehat{\beta}_0$ that solve the

equations (5.9) are:

$$\widehat{\beta}_1 = \frac{\sum_{i=1}^n (x_i - \overline{x})(y_i - \overline{y})}{\sum_{i=1}^n (x_i - \overline{x})^2} \tag{5.40}$$

$$\widehat{\beta}_0 = \overline{y} - \widehat{\beta}_1 \overline{x}, \tag{5.41}$$

provided that not all x_i are the same.

3. Edwin Hubble discovered that the universe is expanding. If v is a galaxy's recession velocity (relative to any other galaxy) and d is its distance (from that same galaxy), Hubble's law states that

$$v = Hd,$$

where H is known as Hubble's constant. The following are distance (in millions of light-years) and velocity (thousands of miles per second) measurements made on five galactic clusters.

distance	68	137	315	405	700
velocity	2.4	4.7	12.0	14.4	26.0

State the regression model and estimate H.

4. The multiple linear regression model (5.6) can be viewed as a first-order approximation of the general model

$$Y = g(\boldsymbol{x}) + \varepsilon, \tag{5.42}$$

where $\mathbb{E}\,\varepsilon = 0$, $\mathbb{V}\mathrm{ar}\,\varepsilon = \sigma^2$, and $g(\boldsymbol{x})$ is some known or unknown function of a d-dimensional vector $\boldsymbol{x}$ of explanatory variables. To see this, replace $g(\boldsymbol{x})$ with its first-order Taylor approximation around some point $\boldsymbol{x}_0$ and write this as $\beta_0 + \boldsymbol{x}^\top \boldsymbol{\beta}$. Express β_0 and $\boldsymbol{\beta}$ in terms of g and $\boldsymbol{x}_0$.

5. Table 5.6 shows data from an agricultural experiment where crop yield was measured for two levels of pesticide and three levels of fertilizer. There are three responses for each combination.

Table 5.6: Crop yields for pesticide and fertilizer combinations.

	Fertilizer		
Pesticide	Low	Medium	High
No	3.23, 3.20, 3.16	2.99, 2.85, 2.77	5.72, 5.77, 5.62
Yes	6.78, 6.73, 6.79	9.07, 9.09, 8.86	8.12, 8.04, 8.31

(a) Organize the data in standard form, where each row corresponds to a single measurement and the columns correspond to the response variable and the two factor variables.

(b) Let Y_{ijk} be the response for the k-th replication at level i for factor 1 and level j for factor 2. To assess which factors best explain the response variable, we use the ANOVA model

$$Y_{ijk} = \mu + \alpha_i + \beta_j + \gamma_{ij} + \varepsilon_{ijk}, \tag{5.43}$$

where $\sum_i \alpha_i = \sum_j \beta_j = \sum_i \gamma_{ij} = \sum_j \gamma_{ij} = 0$. Define $\boldsymbol{\beta} = [\mu, \alpha_1, \alpha_2, \beta_1, \beta_2, \beta_3, \gamma_{11}, \gamma_{12}, \gamma_{13}, \gamma_{21}, \gamma_{22}, \gamma_{23}]^\top$. Give the corresponding 18×12 model matrix.

(c) Note that the parameters are linearly dependent in this case. For example, $\alpha_2 = -\alpha_1$ and $\gamma_{13} = -(\gamma_{11} + \gamma_{12})$. To retain only 6 linearly independent variables consider the 6-dimensional parameter vector $\widetilde{\boldsymbol{\beta}} = [\mu, \alpha_1, \beta_1, \beta_2, \gamma_{11}, \gamma_{12}]^\top$. Find the matrix $\mathbf{M}$ such that $\mathbf{M}\widetilde{\boldsymbol{\beta}} = \boldsymbol{\beta}$.

(d) Give the model matrix corresponding to $\widetilde{\boldsymbol{\beta}}$.

6. Show that for the birthweight data in Section 5.6.6.2 there is no significant decrease in birthweight for smoking mothers. [Hint: create a new variable `nonsmoke` = 1−`smoke`, which reverses the encoding for the smoking and non-smoking mothers. Then, the parameter $\beta_1 + \beta_3$ in the original model is the same as the parameter β_1 in the model

$$\texttt{Bwt} = \beta_0 + \beta_1 \texttt{age} + \beta_2 \texttt{nonsmoke} + \beta_3 \texttt{age} \times \texttt{nonsmoke} + \varepsilon.$$

Now find a 95% for β_3 and see if it contains zero.]

7. Prove (5.37) and (5.38).

8. In the *Tobit regression* model with normally distributed errors, the response is modeled as: TOBIT REGRESSION

$$Y_i = \begin{cases} Z_i, & \text{if } u_i < Z_i \\ u_i, & \text{if } Z_i \leqslant u_i \end{cases}, \qquad \boldsymbol{Z} \sim \mathcal{N}(\mathbf{X}\boldsymbol{\beta}, \sigma^2 \mathbf{I}_n),$$

where the model matrix $\mathbf{X}$ and the thresholds $u_1, \ldots, u_n$ are given. Typically, $u_i = 0, i = 1, \ldots, n$. Suppose we wish to estimate $\boldsymbol{\theta} := (\boldsymbol{\beta}, \sigma^2)$ via the Expectation–Maximization method, similar to the censored data Example 4.2. Let $\boldsymbol{y} = [y_1, \ldots, y_n]^\top$ be the vector of observed data. ☞ 130

(a) Show that the likelihood of $\boldsymbol{y}$ is:

$$g(\boldsymbol{y} \,|\, \boldsymbol{\theta}) = \prod_{i: y_i > u_i} \varphi_{\sigma^2}(y_i - \boldsymbol{x}_i^\top \boldsymbol{\beta}) \times \prod_{i: y_i = u_i} \Phi((u_i - \boldsymbol{x}_i^\top \boldsymbol{\beta})/\sigma),$$

where Φ is the cdf of the $\mathcal{N}(0, 1)$ distribution and φ_{σ^2} the pdf of the $\mathcal{N}(0, \sigma^2)$ distribution.

(b) Let $\overline{\boldsymbol{y}}$ and $\underline{\boldsymbol{y}}$ be vectors that collect all $y_i > u_i$ and $y_i = u_i$, respectively. Denote the corresponding matrix of predictors by $\overline{\mathbf{X}}$ and $\underline{\mathbf{X}}$, respectively. For each observation $y_i = u_i$ introduce a latent variable z_i and collect these into a vector $\boldsymbol{z}$. For the same indices i collect the corresponding u_i into a vector $\boldsymbol{c}$. Show that the complete-data likelihood is given by

$$g(\boldsymbol{y}, \boldsymbol{z} \,|\, \boldsymbol{\theta}) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left(-\frac{\|\overline{\boldsymbol{y}} - \overline{\mathbf{X}}\boldsymbol{\beta}\|^2}{2\sigma^2} - \frac{\|\boldsymbol{z} - \underline{\mathbf{X}}\boldsymbol{\beta}\|^2}{2\sigma^2} \right) \mathbb{1}\{\boldsymbol{z} \leqslant \boldsymbol{c}\}.$$

(c) For the E-step, show that, for a fixed $\boldsymbol{\theta}$,

$$g(\boldsymbol{z} \,|\, \boldsymbol{y}, \boldsymbol{\theta}) = \prod_i g(z_i \,|\, \boldsymbol{y}, \boldsymbol{\theta}),$$

where each $g(z_i \,|\, \boldsymbol{y}, \boldsymbol{\theta})$ is the pdf of the $\mathcal{N}((\underline{\mathbf{X}}\boldsymbol{\beta})_i, \sigma^2)$ distribution, truncated to the interval $(-\infty, c_i]$.

(d) For the M-step, compute the expectation of the complete log-likelihood

$$-\frac{n}{2}\ln\sigma^2 - \frac{n}{2}\ln(2\pi) - \frac{\|\overline{\boldsymbol{y}} - \overline{\mathbf{X}}\boldsymbol{\beta}\|^2}{2\sigma^2} - \frac{\mathbb{E}\|\boldsymbol{Z} - \underline{\mathbf{X}}\boldsymbol{\beta}\|^2}{2\sigma^2}.$$

Then, derive the formulas for $\boldsymbol{\beta}$ and σ^2 that maximize the expectation of the complete log-likelihood.

9. Dowload data set `WomenWage.csv` from the book's website. This data set is a tidied-up version of the women's wages data set from [91]. The first column of the data (`hours`) is the response variable Y. It shows the hours spent in the labor force by married women in the 1970s. We want to understand what factors determine the participation rate of women in the labor force. The predictor variables are:

Table 5.7: Features for the women's wage data set.

Feature	Description
`kidslt6`	Number of children younger than 6 years.
`kidsge6`	Number of children older than 6 years.
`age`	Age of the married woman.
`educ`	Number of years of formal education.
`exper`	Number of years of "work experience".
`nwifeinc`	Non-wife income, that is, the income of the husband.
`expersq`	The square of `exper`, to capture any nonlinear relationships.

We observe that some of the responses are $Y = 0$, that is, some women did not participate in the labor force. For this reason, we model the data using the Tobit regression model, in which the response Y is given as:

$$Y_i = \begin{cases} Z_i, & \text{if } Z_i > 0 \\ 0, & \text{if } Z_i \leqslant 0 \end{cases}, \qquad \boldsymbol{Z} \sim \mathcal{N}(\mathbf{X}\boldsymbol{\beta}, \sigma^2 \mathbf{I}_n).$$

With $\boldsymbol{\theta} = (\boldsymbol{\beta}, \sigma^2)$, the likelihood of the data $\boldsymbol{y} = [y_1, \ldots, y_n]^\top$ is:

$$g(\boldsymbol{y} \,|\, \boldsymbol{\theta}) = \textstyle\prod_{i:y_i>0} \varphi_{\sigma^2}(y_i - \boldsymbol{x}_i^\top \boldsymbol{\beta}) \times \prod_{i:y_i=0} \Phi((u_i - \boldsymbol{x}_i^\top \boldsymbol{\beta})/\sigma),$$

where Φ is the standard normal cdf. In Exercise 8, we derived the EM algorithm for maximizing the log-likelihood.

(a) Write down the EM algorithm in pseudo code as it applies to this Tobit regression.

(b) Implement the EM algorithm pseudo code in Python. Comment on which factor you think is important in determining the labor participation rate of women living in the USA in the 1970s.

10. Let $\mathbf{P}$ be a projection matrix. Show that the diagonal elements of $\mathbf{P}$ all lie in the interval $[0, 1]$. In particular, for $\mathbf{P} = \mathbf{X}\mathbf{X}^+$ in Theorem 5.1, the leverage value $p_i := \mathbf{P}_{ii}$ satisfies $0 \leqslant p_i \leqslant 1$ for all i.

11. Consider the linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$ in (5.8), with $\mathbf{X}$ being the $n \times p$ model matrix and $\boldsymbol{\varepsilon}$ having expectation vector $\mathbf{0}$ and covariance matrix $\sigma^2\mathbf{I}_n$. Suppose that $\widehat{\boldsymbol{\beta}}_{-i}$ is the least-squares estimate obtained by omitting the i-th observation, Y_i; that is,

$$\widehat{\boldsymbol{\beta}}_{-i} = \operatorname*{argmin}_{\boldsymbol{\beta}} \sum_{j \neq i} (Y_j - \boldsymbol{x}_j^\top \boldsymbol{\beta})^2,$$

where $\boldsymbol{x}_j^\top$ is the j-th row of $\mathbf{X}$. Let $\widehat{Y}_{-i} = \boldsymbol{x}_i^\top \widehat{\boldsymbol{\beta}}_{-i}$ be the corresponding fitted value at $\boldsymbol{x}_i$. Also, define $\boldsymbol{B}_i$ as the least-squares estimator of $\boldsymbol{\beta}$ based on the response data

$$\boldsymbol{Y}^{(i)} := [Y_1, \ldots, Y_{i-1}, \widehat{Y}_{-i}, Y_{i+1}, \ldots, Y_n]^\top.$$

(a) Prove that $\widehat{\boldsymbol{\beta}}_{-i} = \boldsymbol{B}_i$; that is, the linear model obtained from fitting all responses except the i-th is the same as the one obtained from fitting the data $\boldsymbol{Y}^{(i)}$.

(b) Use the previous result to verify that

$$Y_i - \widehat{Y}_{-i} = (Y_i - \widehat{Y}_i)/(1 - \mathbf{P}_{ii}),$$

where $\mathbf{P} = \mathbf{X}\mathbf{X}^+$ is the projection matrix onto the columns of $\mathbf{X}$. Hence, deduce the PRESS formula in Theorem 5.1. ☞ 174

12. Take the linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$,where $\mathbf{X}$ is an $n \times p$ model matrix, $\boldsymbol{\varepsilon} = \mathbf{0}$, and $\mathbb{C}\mathrm{ov}(\boldsymbol{\varepsilon}) = \sigma^2\mathbf{I}_n$. Let $\mathbf{P} = \mathbf{X}\mathbf{X}^+$ be the projection matrix onto the columns of $\mathbf{X}$.

(a) Using the properties of the pseudo-inverse (see Definition A.2), show that $\mathbf{P}\mathbf{P}^\top = \mathbf{P}$. ☞ 362

(b) Let $\boldsymbol{E} = \boldsymbol{Y} - \widehat{\boldsymbol{Y}}$ be the (random) vector of residuals, where $\widehat{\boldsymbol{Y}} = \mathbf{P}\boldsymbol{Y}$. Show that the i-th residual has a normal distribution with expectation 0 and variance $\sigma^2(1 - \mathbf{P}_{ii})$ (that is, σ^2 times 1 minus the i-th leverage).

(c) Show that σ^2 can be unbiasedly estimated via

$$S^2 := \frac{1}{n-p}\|\boldsymbol{Y} - \widehat{\boldsymbol{Y}}\|^2 = \frac{1}{n-p}\|\boldsymbol{Y} - \mathbf{X}\widehat{\boldsymbol{\beta}}\|^2. \tag{5.44}$$

[Hint: use the cyclic property of the trace as in Example 2.3.]

13. Consider a normal linear model $\boldsymbol{Y} = \mathbf{X}\boldsymbol{\beta} + \boldsymbol{\varepsilon}$, where $\mathbf{X}$ is an $n \times p$ model matrix and $\boldsymbol{\varepsilon} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_n)$. Exercise 12 shows that for any such model the i-th standardized residual $E_i/(\sigma\sqrt{1 - \mathbf{P}_{ii}})$ has a standard normal distribution. This motivates the use of the leverage $\mathbf{P}_{ii}$ to assess whether the i-th observation is an outlier depending on the size of the i-th residual relative to $\sqrt{1 - \mathbf{P}_{ii}}$. A more robust approach is to include an estimate for σ using

STUDENTIZED RESIDUAL

all data except the i-th observation. This gives rise to the *studentized residual* T_i, defined as

$$T_i := \frac{E_i}{S_{-i}\sqrt{1-\mathbf{P}_{ii}}},$$

where S_{-i} is an estimate of σ obtained by fitting all the observations except the i-th and $E_i = Y_i - \widehat{Y}_i$ is the i-th (random) residual. Exercise 12 shows that we can take, for example,

$$S_{-i}^2 = \frac{1}{n-1-p}\|\boldsymbol{Y}_{-i} - \mathbf{X}_{-i}\widehat{\boldsymbol{\beta}}_{-i}\|^2, \tag{5.45}$$

where $\mathbf{X}_{-i}$ is the model matrix $\mathbf{X}$ with the i-th row removed, is an unbiased estimator of σ^2. We wish to compute S_{-i}^2 efficiently, using S^2 in (5.44), as the latter will typically be available once we have fitted the linear model. To this end, define $\boldsymbol{u}_i$ as the i-th unit vector $[0,\ldots,0,1,0,\ldots,0]^\top$, and let

$$\boldsymbol{Y}^{(i)} := \boldsymbol{Y} - (Y_i - \widehat{Y}_{-i})\boldsymbol{u}_i = \boldsymbol{Y} - \frac{E_i}{1-\mathbf{P}_{ii}}\boldsymbol{u}_i,$$

where we have used the fact that $Y_i - \widehat{Y}_{-i} = E_i/(1-\mathbf{P}_{ii})$, as derived in the proof of Theorem 5.1. Now apply Exercise 11 to prove that

$$S_{-i}^2 = \frac{(n-p)\,S^2 - E_i^2/(1-\mathbf{P}_{ii})}{n-p-1}.$$

COOK'S DISTANCE

14. Using the notation from Exercises 11–13, *Cook's distance* for observation i is defined as

$$D_i := \frac{\|\widehat{\boldsymbol{Y}} - \widehat{\boldsymbol{Y}}^{(i)}\|^2}{p\,S^2}.$$

It measures the change in the fitted values when the i-th observation is removed, relative to the residual variance of the model (estimated via S^2).

By using similar arguments as those in Exercise 13, show that

$$D_i = \frac{\mathbf{P}_{ii}\,E_i^2}{(1-\mathbf{P}_{ii})^2 p\,S^2}.$$

It follows that there is no need to "omit and refit" the linear model in order to compute Cook's distance for the i-th response.

15. Prove that if we add an additional feature to the general linear model, then R^2, the coefficient of determination, is necessarily non-decreasing in value and hence cannot be used to compare models with different numbers of predictors.

16. Let $\boldsymbol{X} := [X_1,\ldots,X_n]^\top$ and $\boldsymbol{\mu} := [\mu_1,\ldots,\mu_n]^\top$. In the fundamental Theorem C.9, we use the fact that if $X_i \sim \mathcal{N}(\mu_i, 1)$, $i = 1,\ldots,n$ are independent, then $\|\boldsymbol{X}\|^2$ has (per definition) a noncentral χ_n^2 distribution. Show that $\|\boldsymbol{X}\|^2$ has moment generating function

$$\frac{\mathrm{e}^{t\|\boldsymbol{\mu}\|^2/(1-2t)}}{(1-2t)^{n/2}}, \quad t < 1/2,$$

and so the distribution of $\|\boldsymbol{X}\|^2$ depends on $\boldsymbol{\mu}$ only through the norm $\|\boldsymbol{\mu}\|$.

17. Carry out a logistic regression analysis on a (partial) *wine* data set classification problem. The data can be loaded using the following code.

```
from sklearn import datasets
import numpy as np
data = datasets.load_wine()
X = data.data[:, [9,10]]
y = np.array(data.target==1,dtype=np.uint)
X = np.append(np.ones(len(X)).reshape(-1,1),X,axis=1)
```

The model matrix has three features, including the constant feature. Instead of using Newton's method (5.39) to estimate $\boldsymbol{\beta}$, implement a simple gradient descent procedure

$$\boldsymbol{\beta}_t = \boldsymbol{\beta}_{t-1} - \alpha \nabla r_\tau(\boldsymbol{\beta}_{t-1}),$$

with learning rate $\alpha = 0.0001$, and run it for 10^6 steps. Your procedure should deliver three coefficients; one for the intercept and the rest for the explanatory variables. Solve the same problem using the `Logit` method of `statsmodels.api` and compare the results.

18. Consider again Example 5.10, where we train the learner via the Newton iteration (5.39). If $\mathbf{X}^\top := [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$ defines the matrix of predictors and $\boldsymbol{\mu}_t := \boldsymbol{h}(\mathbf{X}\boldsymbol{\beta}_t)$, then the gradient (5.37) and Hessian (5.38) for Newton's method can be written as: ☞ 205

$$\nabla r_\tau(\boldsymbol{\beta}_t) = \frac{1}{n}\mathbf{X}^\top(\boldsymbol{\mu}_t - \boldsymbol{y}) \quad \text{and} \quad \mathbf{H}(\boldsymbol{\beta}_t) = \frac{1}{n}\mathbf{X}^\top \mathbf{D}_t \mathbf{X},$$

where $\mathbf{D}_t := \operatorname{diag}(\boldsymbol{\mu}_t \odot (\mathbf{1} - \boldsymbol{\mu}_t))$ is a diagonal matrix. Show that the Newton iteration (5.39) can be written as the *iterative reweighted least-squares* method:

ITERATIVE REWEIGHTED LEAST SQUARES

$$\boldsymbol{\beta}_t = \operatorname*{argmin}_{\boldsymbol{\beta}} (\widetilde{\boldsymbol{y}}_{t-1} - \mathbf{X}\boldsymbol{\beta})^\top \mathbf{D}_{t-1} (\widetilde{\boldsymbol{y}}_{t-1} - \mathbf{X}\boldsymbol{\beta}),$$

where $\widetilde{\boldsymbol{y}}_{t-1} := \mathbf{X}\boldsymbol{\beta}_{t-1} + \mathbf{D}_{t-1}^{-1}(\boldsymbol{y} - \boldsymbol{\mu}_{t-1})$ is the so-called *adjusted response*. [Hint: use the fact that $(\mathbf{M}^\top\mathbf{M})^{-1}\mathbf{M}^\top \boldsymbol{z}$ is the minimizer of $\|\mathbf{M}\boldsymbol{\beta} - \boldsymbol{z}\|^2$.]

19. In *multi-output linear regression*, the response variable is a real-valued vector of dimension, say, m. Similar to (5.8), the model can be written in matrix notation:

MULTI-OUTPUT LINEAR REGRESSION

$$\mathbf{Y} = \mathbf{X}\mathbf{B} + \begin{bmatrix} \boldsymbol{\varepsilon}_1^\top \\ \vdots \\ \boldsymbol{\varepsilon}_n^\top \end{bmatrix},$$

where:

- $\mathbf{Y}$ is an $n \times m$ matrix of n independent responses (stored as row vectors of length m);
- $\mathbf{X}$ is the usual $n \times p$ model matrix;
- $\mathbf{B}$ is an $p \times m$ matrix of model parameters;
- $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_n \in \mathbb{R}^m$ are independent error terms with $\mathbb{E}\,\boldsymbol{\varepsilon} = \mathbf{0}$ and $\mathbb{E}\,\boldsymbol{\varepsilon}\boldsymbol{\varepsilon}^\top = \boldsymbol{\Sigma}$.

We wish to learn the matrix parameters $\mathbf{B}$ and $\mathbf{\Sigma}$ from the training set $\{\mathbf{Y}, \mathbf{X}\}$. To this end, consider minimizing the training loss:

$$\frac{1}{n}\mathrm{tr}\left((\mathbf{Y}-\mathbf{X}\mathbf{B})\,\mathbf{\Sigma}^{-1}\,(\mathbf{Y}-\mathbf{X}\mathbf{B})^\top\right),$$

☞ 359 where $\mathrm{tr}(\cdot)$ is the trace of a matrix.

(a) Show that the minimizer of the training loss, denoted $\widehat{\mathbf{B}}$, satisfies the normal equations:

$$\mathbf{X}^\top\mathbf{X}\,\widehat{\mathbf{B}} = \mathbf{X}^\top\mathbf{Y}.$$

(b) Noting that

$$(\mathbf{Y}-\mathbf{X}\mathbf{B})^\top(\mathbf{Y}-\mathbf{X}\mathbf{B}) = \sum_{i=1}^{n}\boldsymbol{\varepsilon}_i\boldsymbol{\varepsilon}_i^\top,$$

explain why

$$\widehat{\mathbf{\Sigma}} := \frac{(\mathbf{Y}-\mathbf{X}\widehat{\mathbf{B}})^\top(\mathbf{Y}-\mathbf{X}\widehat{\mathbf{B}})}{n}$$

is a method-of-moments estimator of $\mathbf{\Sigma}$, just like the one given in (5.10).

CHAPTER 6

REGULARIZATION AND KERNEL METHODS

The purpose of this chapter is to familiarize the reader with two central concepts in modern data science and machine learning: regularization and kernel methods. Regularization provides a natural way to guard against overfitting and kernel methods offer a broad generalization of linear models. Here, we discuss regularized regression (ridge, lasso) as a bridge to the fundamentals of kernel methods. We introduce reproducing kernel Hilbert spaces and show that selecting the best prediction function in such spaces is in fact a finite-dimensional optimization problem. Applications to spline fitting, Gaussian process regression, and kernel PCA are given.

6.1 Introduction

In this chapter we return to the supervised learning setting of Chapter 5 (regression) and expand its scope. Given training data $\tau = \{(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)\}$, we wish to find a prediction function (the learner) g_τ that minimizes the (squared-error) training loss

$$\ell_\tau(g) = \frac{1}{n}\sum_{i=1}^{n}(y_i - g(\boldsymbol{x}_i))^2$$

within a class of functions $\mathcal{G}$. As noted in Chapter 2, if $\mathcal{G}$ is the set of all possible functions then choosing *any* function g with the property that $g(\boldsymbol{x}_i) = y_i$ for all i will give zero training loss, but will likely have poor generalization performance (that is, suffer from overfitting).

Recall from Theorem 2.1 that the best possible prediction function (over all g) for the squared-error *risk* $\mathbb{E}(Y - g(\boldsymbol{X}))^2$ is given by $g^*(\boldsymbol{x}) = \mathbb{E}[Y \mid \boldsymbol{X} = \boldsymbol{x}]$. The class $\mathcal{G}$ should be simple enough to permit theoretical understanding and analysis but, at the same time, rich enough to contain the optimal function g^* (or a function close to g^*). This ideal can be realized by taking $\mathcal{G}$ to be a *Hilbert space* (i.e., a complete inner product space) of functions; see Appendix A.7.

☞ 21

HILBERT SPACE

☞ 386

Many of the classes of functions that we have encountered so far are in fact Hilbert spaces. In particular, the set $\mathcal{G}$ of *linear* functions on $\mathbb{R}^p$ is a Hilbert space. To see this,

identify with each element $\boldsymbol{\beta} \in \mathbb{R}^p$ the linear function $g_\beta : \boldsymbol{x} \mapsto \boldsymbol{x}^\top \boldsymbol{\beta}$ and define the inner product on $\mathcal{G}$ as $\langle g_\beta, g_\gamma \rangle := \boldsymbol{\beta}^\top \boldsymbol{\gamma}$. In this way, $\mathcal{G}$ behaves in exactly the same way as (is isomorphic to) the space $\mathbb{R}^p$ equipped with the Euclidean inner product (dot product). The latter is a Hilbert space, because it is *complete* with respect to the Euclidean norm. See Exercise 12 for a further discussion.

☞ 362

COMPLETE VECTOR SPACE

☞ 26

Let us now turn to our "running" polynomial regression Example 2.1, where the feature vector $\boldsymbol{x} = [1, u, u^2, \ldots, u^{p-1}]^\top =: \boldsymbol{\phi}(u)$ is itself a vector-valued function of another feature u. Then, the space of functions $h_\beta : u \mapsto \boldsymbol{\phi}(u)^\top \boldsymbol{\beta}$ is a Hilbert space, through the identification $h_\beta \equiv \boldsymbol{\beta}$. In fact, this is true for *any* feature mapping $\boldsymbol{\phi} : u \mapsto [\phi_1(u), \ldots, \phi_p(u)]^\top$.

FEATURE MAPS

This can be further generalized by considering *feature maps* $u \mapsto \kappa_u$, where each κ_u is a real-valued *function* $v \mapsto \kappa_u(v)$ on the feature space. As we shall soon see (in Section 6.3), functions of the form $u \mapsto \sum_{i=1}^{\infty} \beta_i \kappa_{v_i}(u)$ live in a Hilbert space of functions called a *reproducing kernel Hilbert space* (RKHS). In Section 6.3 we introduce the notion of a RKHS formally, give specific examples, including the linear and Gaussian kernels, and derive various useful properties, the most important of which is the representer Theorem 6.6. Applications of such spaces include the *smoothing splines* (Section 6.6), Gaussian process regression (Section 6.7), kernel PCA (Section 6.8), and *support vector machines* for classification (Section 7.7).

RKHS

☞ 235

☞ 271

REGULARIZATION

The RKHS formalism also makes it easier to treat the important topic of *regularization*. The aim of regularization is to improve the predictive performance of the best learner in some class of functions $\mathcal{G}$ by adding a penalty term to the training loss that penalizes learners that tend to overfit the data. In the next section we introduce the main ideas behind regularization, which then segues into a discussion of kernel methods in the subsequent sections.

6.2 Regularization

Let $\mathcal{G}$ be the Hilbert space of functions over which we search for the minimizer, g_τ, of the training loss $\ell_\tau(g)$. Often, the Hilbert space $\mathcal{G}$ is rich enough so that we can find a learner g_τ within $\mathcal{G}$ such that the training loss is zero or close to zero. Consequently, if the space of functions $\mathcal{G}$ is sufficiently rich, we run the risk of overfitting. One way to avoid overfitting is to restrict attention to a subset of the space $\mathcal{G}$ by introducing a non-negative functional $J : \mathcal{G} \to \mathbb{R}_+$ which penalizes complex models (functions). In particular, we want to find functions $g \in \mathcal{G}$ such that $J(g) < c$ for some "regularization" constant $c > 0$. Thus we can formulate the quintessential supervised learning problem as:

$$\min \{\ell_\tau(g) \ : \ g \in \mathcal{G}, J(g) < c\}, \tag{6.1}$$

the solution (argmin) of which is our learner. When this optimization problem is convex, it can be solved by first obtaining the Lagrangian dual function

$$\mathcal{L}^*(\lambda) := \min_{g \in \mathcal{G}} \{\ell_\tau(g) + \lambda(J(g) - c)\},$$

☞ 409

and then maximizing $\mathcal{L}^*(\lambda)$ with respect to $\lambda \geqslant 0$; see Section B.2.3.

In order to introduce the overall ideas of kernel methods and regularization, we will proceed by exploring (6.1) in the special case of *ridge regression*, with the following running example.

RIDGE REGRESSION

■ **Example 6.1 (Ridge Regression)** *Ridge regression* is simply linear regression with a squared-norm penalty functional (also called a regularization function, or *regularizer*). Suppose we have a training set $\tau = \{(\boldsymbol{x}_i, y_i), i = 1, \ldots, n\}$, with each $\boldsymbol{x}_i \in \mathbb{R}^p$ and we use a squared-norm penalty with *regularization parameter* $\gamma > 0$. Then, the problem is to solve

REGULARIZER

REGULARIZATION PARAMETER

$$\min_{g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^{n} (y_i - g(\boldsymbol{x}_i))^2 + \gamma \, \|g\|^2, \tag{6.2}$$

where $\mathcal{G}$ is the Hilbert space of linear functions on $\mathbb{R}^p$. As explained in Section 6.1, we can identify each $g \in \mathcal{G}$ with a vector $\boldsymbol{\beta} \in \mathbb{R}^p$ and, consequently, $\|g\|^2 = \langle \boldsymbol{\beta}, \boldsymbol{\beta} \rangle = \|\boldsymbol{\beta}\|^2$. The above *functional* optimization problem is thus equivalent to the *parametric* optimization problem

$$\min_{\boldsymbol{\beta} \in \mathbb{R}^p} \frac{1}{n} \sum_{i=1}^{n} (y_i - \boldsymbol{x}_i^\top \boldsymbol{\beta})^2 + \gamma \, \|\boldsymbol{\beta}\|^2, \tag{6.3}$$

which, in the notation of Chapter 5, further simplifies to

$$\min_{\boldsymbol{\beta} \in \mathbb{R}^p} \frac{1}{n} \| \boldsymbol{y} - \mathbf{X}\boldsymbol{\beta} \|^2 + \gamma \, \|\boldsymbol{\beta}\|^2. \tag{6.4}$$

In other words, the solution to (6.2) is of the form $\boldsymbol{x} \mapsto \boldsymbol{x}^\top \boldsymbol{\beta}^*$, where $\boldsymbol{\beta}^*$ solves (6.3) (or equivalently (6.4)). Observe that as $\gamma \to \infty$, the regularization term becomes dominant and consequently the optimal g becomes identically zero.

The optimization problem in (6.4) is convex, and by multiplying by the constant $n/2$ and setting the gradient equal to zero, we obtain

$$\mathbf{X}^\top (\mathbf{X}\boldsymbol{\beta} - \boldsymbol{y}) + n \, \gamma \, \boldsymbol{\beta} = \mathbf{0}. \tag{6.5}$$

If $\gamma = 0$ these are simply the *normal equations*, albeit written in a slightly different form. If the matrix $\mathbf{X}^\top \mathbf{X} + n \, \gamma \mathbf{I}_p$ is invertible (which is the case for any $\gamma > 0$; see Exercise 13), then the solution to these modified normal equations is

☞ 28

$$\widehat{\boldsymbol{\beta}} = (\mathbf{X}^\top \mathbf{X} + n \, \gamma \mathbf{I}_p)^{-1} \mathbf{X}^\top \boldsymbol{y}.$$

■

When using regularization with respect to some Hilbert space $\mathcal{G}$, it is sometimes useful to decompose $\mathcal{G}$ into two orthogonal subspaces, $\mathcal{H}$ and $\mathcal{C}$ say, such that every $g \in \mathcal{G}$ can be uniquely written as $g = h + c$, with $h \in \mathcal{H}$, $c \in \mathcal{C}$, and $\langle h, c \rangle = 0$. Such a $\mathcal{G}$ is said to be the *direct sum* of $\mathcal{C}$ and $\mathcal{H}$, and we write $\mathcal{G} = \mathcal{H} \oplus \mathcal{C}$. Decompositions of this form become useful when functions in $\mathcal{H}$ are penalized but functions in $\mathcal{C}$ are not. We illustrate this decomposition with the ridge regression example where one of the features is a constant term, which we do not wish to penalize.

DIRECT SUM

■ **Example 6.2 (Ridge Regression (cont.))** Suppose one of the features in Example 6.1 is the constant 1, which we do not wish to penalize. The reason for this is to ensure that when $\gamma \to \infty$, the optimal g becomes the "constant" model, $g(\boldsymbol{x}) = \beta_0$, rather than the "zero" model, $g(\boldsymbol{x}) = 0$. Let us alter the notation slightly by considering the feature vectors to be of the form $\widetilde{\boldsymbol{x}} = [1, \boldsymbol{x}^\top]^\top$, where $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$. We thus have $p + 1$ features, rather

than p. Let $\mathcal{G}$ be the space of linear functions of $\widetilde{\boldsymbol{x}}$. Each linear function g of $\widetilde{\boldsymbol{x}}$ can be written as $g : \widetilde{\boldsymbol{x}} \mapsto \beta_0 + \boldsymbol{x}^\top \boldsymbol{\beta}$, which is the sum of the constant function $c : \widetilde{\boldsymbol{x}} \mapsto \beta_0$ and $h : \widetilde{\boldsymbol{x}} \mapsto \boldsymbol{x}^\top \boldsymbol{\beta}$. Moreover, the two functions are orthogonal with respect to the inner product on $\mathcal{G}$: $\langle c, h \rangle = [\beta_0, \mathbf{0}^\top][0, \boldsymbol{\beta}^\top]^\top = 0$, where $\mathbf{0}$ is a column vector of zeros.

As subspaces of $\mathcal{G}$, both $\mathcal{C}$ and $\mathcal{H}$ are again Hilbert spaces, and their inner products and norms follow directly from the inner product on $\mathcal{G}$. For example, each function $h : \widetilde{\boldsymbol{x}} \mapsto \boldsymbol{x}^\top \boldsymbol{\beta}$ in $\mathcal{H}$ has norm $\|h\|_{\mathcal{H}} = \|\boldsymbol{\beta}\|$, and the constant function $c : \widetilde{\boldsymbol{x}} \mapsto \beta_0$ in $\mathcal{C}$ has norm $|\beta_0|$.

The modification of the regularized optimization problem (6.2) where the constant term is not penalized can now be written as

$$\min_{g \in \mathcal{H} \oplus \mathcal{C}} \frac{1}{n} \sum_{i=1}^{n} (y_i - g(\widetilde{\boldsymbol{x}}_i))^2 + \gamma \, \|g\|_{\mathcal{H}}^2, \tag{6.6}$$

which further simplifies to

$$\min_{\beta_0, \boldsymbol{\beta}} \frac{1}{n} \| \boldsymbol{y} - \beta_0 \mathbf{1} - \mathbf{X}\boldsymbol{\beta} \|^2 + \gamma \, \|\boldsymbol{\beta}\|^2, \tag{6.7}$$

where $\mathbf{1}$ is the $n \times 1$ vector of 1s. Observe that, in this case, as $\gamma \to \infty$ the optimal g tends to the sample mean $\bar{y}$ of the $\{y_i\}$; that is, we obtain the "default" regression model, without explanatory variables. Again, this is a convex optimization problem, and the solution follows from

$$\mathbf{X}^\top (\beta_0 \mathbf{1} + \mathbf{X}\boldsymbol{\beta} - \boldsymbol{y}) + n \gamma \boldsymbol{\beta} = \mathbf{0}, \tag{6.8}$$

with

$$n \beta_0 = \mathbf{1}^\top (\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}). \tag{6.9}$$

This results in solving for $\boldsymbol{\beta}$ from

$$(\mathbf{X}^\top \mathbf{X} - n^{-1} \mathbf{X}^\top \mathbf{1}\mathbf{1}^\top \mathbf{X} + n \gamma \mathbf{I}_p) \boldsymbol{\beta} = (\mathbf{X}^\top - n^{-1} \mathbf{X}^\top \mathbf{1}\mathbf{1}^\top) \boldsymbol{y}, \tag{6.10}$$

and determining β_0 from (6.9).

As a precursor to the kernel methods in the following sections, let us assume that $n \geqslant p$ and that $\mathbf{X}$ has full (column) rank p. Then any vector $\boldsymbol{\beta} \in \mathbb{R}^p$ can be written as a linear combination of the feature vectors $\{\boldsymbol{x}_i\}$; that is, as linear combinations of the columns of the matrix $\mathbf{X}^\top$. In particular, let $\boldsymbol{\beta} = \mathbf{X}^\top \boldsymbol{\alpha}$, where $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]^\top \in \mathbb{R}^n$. In this case (6.10) reduces to

$$(\mathbf{X}\mathbf{X}^\top - n^{-1} \mathbf{1}\mathbf{1}^\top \mathbf{X}\mathbf{X}^\top + n \gamma \mathbf{I}_n) \boldsymbol{\alpha} = (\mathbf{I}_n - n^{-1} \mathbf{1}\mathbf{1}^\top) \boldsymbol{y}.$$

Assuming invertibility of $(\mathbf{X}\mathbf{X}^\top - n^{-1} \mathbf{1}\mathbf{1}^\top \mathbf{X}\mathbf{X}^\top + n \gamma \mathbf{I}_n)$, we have the solution

$$\widehat{\boldsymbol{\alpha}} = (\mathbf{X}\mathbf{X}^\top - n^{-1} \mathbf{1}\mathbf{1}^\top \mathbf{X}\mathbf{X}^\top + n \gamma \mathbf{I}_n)^{-1} (\mathbf{I}_n - n^{-1} \mathbf{1}\mathbf{1}^\top) \boldsymbol{y},$$

which depends on the training feature vectors $\{\boldsymbol{x}_i\}$ only through the $n \times n$ matrix of inner products: $\mathbf{X}\mathbf{X}^\top = [\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle]$. This matrix is called the *Gram matrix* of the $\{\boldsymbol{x}_i\}$. From (6.9), the solution for the constant term is $\widehat{\beta_0} = n^{-1} \mathbf{1}^\top (\boldsymbol{y} - \mathbf{X}\mathbf{X}^\top \widehat{\boldsymbol{\alpha}})$. It follows that the learner is a linear combination of inner products $\{\langle \boldsymbol{x}_i, \boldsymbol{x} \rangle\}$ plus a constant:

Gram matrix

$$g_\tau(\widetilde{\boldsymbol{x}}) = \widehat{\beta_0} + \boldsymbol{x}^\top \mathbf{X}^\top \widehat{\boldsymbol{\alpha}} = \widehat{\beta_0} + \sum_{i=1}^{n} \widehat{\alpha_i} \, \langle \boldsymbol{x}_i, \boldsymbol{x} \rangle,$$

where the coefficients $\widehat{\beta}_0$ and $\widehat{\boldsymbol{\alpha}}_i$ only depend on the inner products $\{\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle\}$. We will see shortly that the representer Theorem 6.6 generalizes this result to a broad class of regularized optimization problems. ■

☞ 232

We illustrate in Figure 6.1 how the solutions of the ridge regression problems appearing in Examples 6.1 and 6.2 are qualitatively affected by the regularization parameter γ for a simple linear regression model. The data was generated from the model $y_i = -1.5 + 0.5x_i + \varepsilon_i$, $i = 1, \ldots, 100$, where each x_i is drawn independently and uniformly from the interval $[0, 10]$ and each ε_i is drawn independently from the standard normal distribution.

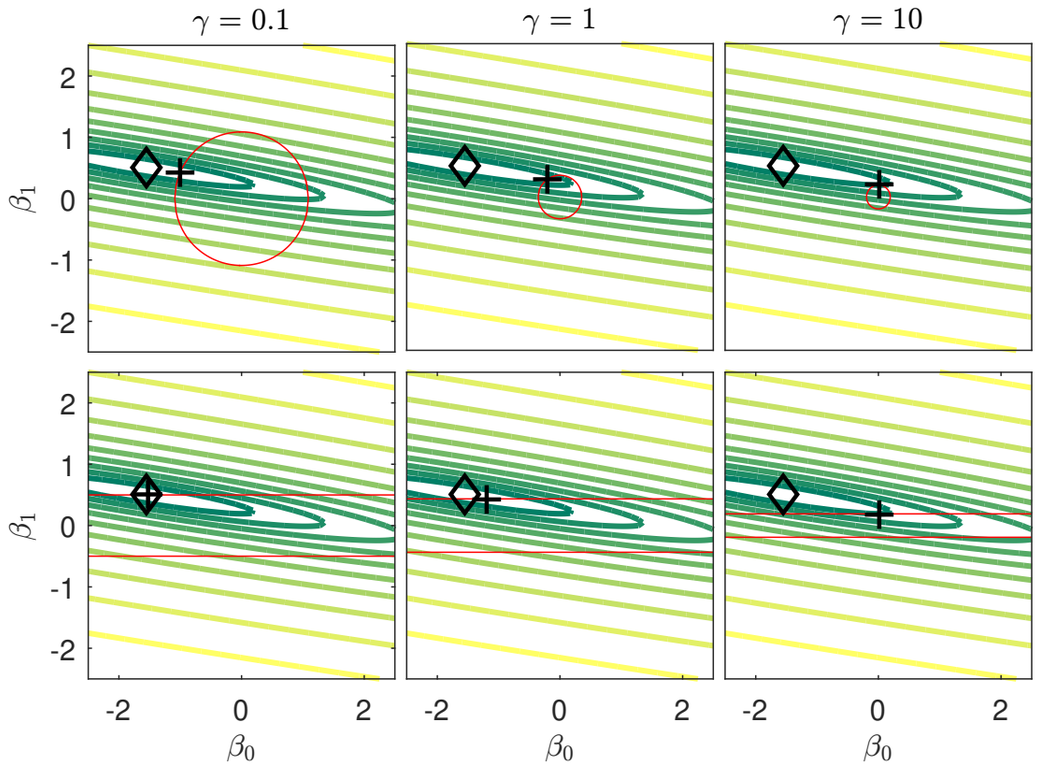


Figure 6.1: Ridge regression solutions for a simple linear regression problem. Each panel shows contours of the loss function (log scale) and the effect of the regularization parameter $\gamma \in \{0.1, 1, 10\}$, appearing in (6.4) and (6.7). Top row: both terms are penalized. Bottom row: only the non-constant term is penalized. Penalized (plus) and unpenalized (diamond) solutions are shown in each case.

The contours are those of the squared-error loss (actually the logarithm thereof), which is minimized with respect to the model parameters β_0 and β_1. The diamonds all represent the same minimizer of this loss. The plusses show each minimizer $[\beta_0^*, \beta_1^*]^\top$ of the regularized minimization problems (6.4) and (6.7) for three choices of the regularization parameter γ. For the top three panels the regularization involves both β_0 and β_1, through the squared norm $\beta_0^2 + \beta_1^2$. The circles show the points that have the same squared norm as

the optimal solution. For the bottom three panels only β_1 is regularized; there, horizontal lines indicate vectors $[\beta_0, \beta_1]^\top$ for which $|\beta_1| = |\beta_1^*|$.

The problem of ridge regression discussed in Example 6.2 boils down to solving a problem of the form in (6.7), involving a squared 2-norm penalty $\|\boldsymbol{\beta}\|^2$. A natural question to ask is whether we can replace the squared 2-norm penalty by a different penalty term. Replacing it with a 1-norm gives the *lasso* (least absolute shrinkage and selection operator). The lasso equivalent of the ridge regression problem (6.7) is thus:

☞ 410
LASSO

$$\min_{\beta_0, \boldsymbol{\beta}} \frac{1}{n} \| \boldsymbol{y} - \beta_0 \mathbf{1} - \mathbf{X}\boldsymbol{\beta} \|^2 + \gamma \|\boldsymbol{\beta}\|_1, \tag{6.11}$$

where $\|\boldsymbol{\beta}\|_1 = \sum_{i=1}^{p} |\beta_i|$.

This is again a convex optimization problem. Unlike ridge regression, the lasso generally does not have an explicit solution, and so numerical methods must be used to solve it. Note that the problem (6.11) is of the form

$$\begin{aligned} \min_{\boldsymbol{x}, \boldsymbol{z}} \quad & f(\boldsymbol{x}) + g(\boldsymbol{z}) \\ \text{subject to} \quad & \mathbf{A}\boldsymbol{x} + \mathbf{B}\boldsymbol{z} = \boldsymbol{c}, \end{aligned} \tag{6.12}$$

with $\boldsymbol{x} := [\beta_0, \boldsymbol{\beta}^\top]^\top$, $\boldsymbol{z} := \boldsymbol{\beta}$, $\mathbf{A} := [\mathbf{0}_p, \mathbf{I}_p]$, $\mathbf{B} := -\mathbf{I}_p$, and $\boldsymbol{c} := \mathbf{0}_p$ (vector of zeros), and convex functions $f(\boldsymbol{x}) := \frac{1}{n} \| \boldsymbol{y} - [\mathbf{1}_n, \mathbf{X}]\, \boldsymbol{x} \|^2$ and $g(\boldsymbol{z}) := \gamma \|\boldsymbol{z}\|_1$. There exist efficient algorithms for solving such problems, including the *alternating direction method of multipliers* (ADMM) [17]. We refer to Example **??** for details on this algorithm.

☞ 418

We repeat the examples from Figure 6.1, but now using lasso regression and taking the square roots of the previous regularization parameters. The results are displayed in Figure 6.2.

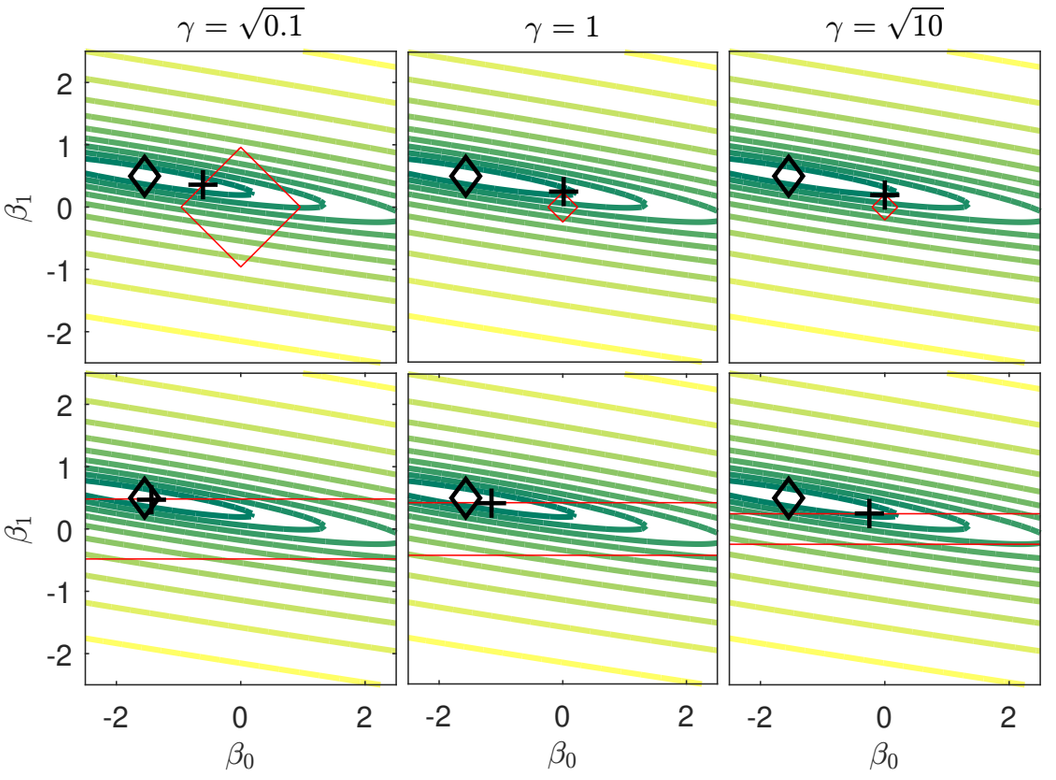


Figure 6.2: Lasso regression solutions. Compare with Figure 6.1.

One advantage of using the lasso regularization is that the resulting optimal parameter vector often has several components that are exactly 0. For example, in the top middle and right panels of Figure 6.2, the optimal solution lies exactly at a corner point of the square $\{[\beta_0, \beta_1]^\top : |\beta_0| + |\beta_1| = |\beta_0^*| + |\beta_1^*|\}$; in this case $\beta_0^* = 0$. For statistical models with many parameters, the lasso can provide a methodology for model selection. Namely, as the regularization parameter increases (or, equivalently, as the L_1 norm of the optimal solution decreases), the solution vector will have fewer and fewer non-zero parameters. By plotting the values of the parameters for each γ or L_1 one obtains the so-called *regularization paths* (also called *homotopy paths* or *coefficient profiles*) for the variables. Inspection of such paths may help assess which of the model parameters are relevant to explain the variability in the observed responses $\{y_i\}$.

REGULARIZATION PATHS

■ **Example 6.3 (Regularization Paths)** Figure 6.3 shows the regularization paths for $p = 60$ coefficients from a multiple linear regression model

☞ 169

$$Y_i = \sum_{j=1}^{60} \beta_j x_{ij} + \varepsilon_i, \quad i = 1, \ldots, 150,$$

where $\beta_j = 1$ for $j = 1, \ldots, 10$ and $\beta_j = 0$ for $j = 11, \ldots, 60$. The error terms $\{\varepsilon_i\}$ are independent and standard normal. The explanatory variables $\{x_{ij}\}$ were independently generated from a standard normal distribution. As it is clear from the figure, the estimates of the 10

non-zero coefficients are first selected, as the L_1 norm of the solutions increases. By the time the L_1 norm reaches around 4, all 10 variables for which $\beta_j = 1$ have been correctly identified and the remaining 50 parameters are estimated as exactly 0. Only after the L_1 norm reaches around 8, will these "spurious" parameters be estimated to be non-zero. For this example, the regularization parameter γ varied from 10^{-4} to 10.

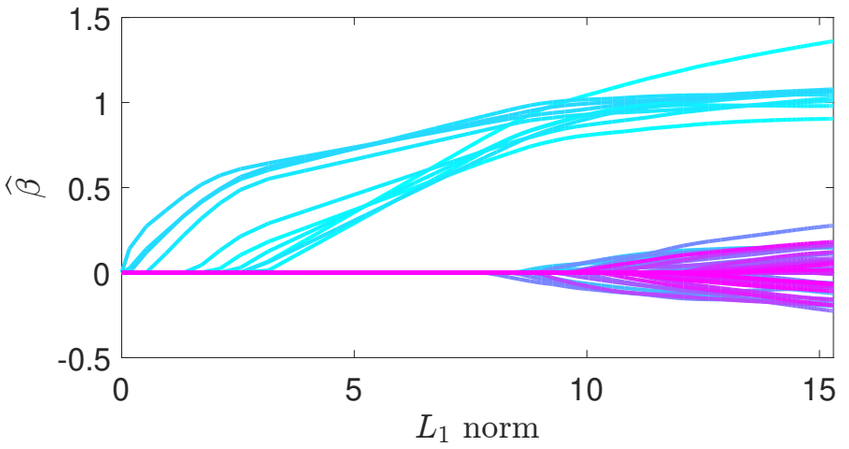


Figure 6.3: Regularization paths for lasso regression solutions as a function of the L_1 norm of the solutions.

6.3 Reproducing Kernel Hilbert Spaces

In this section, we formalize the idea outlined at the end of Section 6.1 of extending finite dimensional feature maps to those that are *functions* by introducing a special type of Hilbert space of functions known as a *reproducing kernel Hilbert space* (RKHS). Although the theory extends naturally to Hilbert spaces of complex-valued functions, we restrict attention to Hilbert spaces of real-valued functions here.

To evaluate the loss of a learner g in some class of functions $\mathcal{G}$, we do not need to explicitly construct g — rather, it is only required that we can evaluate g at all the feature vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ of the training set. A defining property of an RKHS is that function evaluation at a point $\boldsymbol{x}$ can be performed by simply taking the inner product of g with some feature function $\kappa_{\boldsymbol{x}}$ associated with $\boldsymbol{x}$. We will see that this property becomes particularly useful in light of the representer theorem (see Section 6.5), which states that the learner g itself can be represented as a linear combination of the set of feature functions $\{\kappa_{\boldsymbol{x}_i}, i = 1, \ldots, n\}$. Consequently, we can evaluate a learner g at the feature vectors $\{\boldsymbol{x}_i\}$ by taking linear combinations of terms of the form $\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) = \langle \kappa_{\boldsymbol{x}_i}, \kappa_{\boldsymbol{x}_j} \rangle_{\mathcal{G}}$. Collecting these inner products into a matrix $\mathbf{K} = [\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j), i, j = 1, \ldots, n]$ (the Gram matrix of the $\{\kappa_{\boldsymbol{x}_i}\}$), we will see that the feature vectors $\{\boldsymbol{x}_i\}$ only enter the loss minimization problem through $\mathbf{K}$.

☞ 231

Definition 6.1: Reproducing Kernel Hilbert Space

For a non-empty set $\mathcal{X}$, a Hilbert space $\mathcal{G}$ of functions $g : \mathcal{X} \to \mathbb{R}$ with inner product $\langle \cdot, \cdot \rangle_{\mathcal{G}}$ is called a *reproducing kernel Hilbert space* (RKHS) with *reproducing kernel* $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ if:

REPRODUCING KERNEL HILBERT SPACE

1. for every $\boldsymbol{x} \in \mathcal{X}$, $\kappa_{\boldsymbol{x}} := \kappa(\boldsymbol{x}, \cdot)$ is in $\mathcal{G}$,
2. $\kappa(\boldsymbol{x}, \boldsymbol{x}) < \infty$ for all $\boldsymbol{x} \in \mathcal{X}$,
3. for every $\boldsymbol{x} \in \mathcal{X}$ and $g \in \mathcal{G}$, $g(\boldsymbol{x}) = \langle g, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}}$.

The reproducing kernel of a Hilbert space of functions, if it exists, is unique; see Exercise 2. The main (third) condition in Definition 6.1 is known as the *reproducing property*. This property allows us to evaluate any function $g \in \mathcal{G}$ at a point $\boldsymbol{x} \in \mathcal{X}$ by taking the inner product of g and $\kappa_{\boldsymbol{x}}$; as such, $\kappa_{\boldsymbol{x}}$ is called the *representer of evaluation*. Further, by taking $g = \kappa_{\boldsymbol{x}'}$ and applying the reproducing property, we have $\langle \kappa_{\boldsymbol{x}'}, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}} = \kappa(\boldsymbol{x}', \boldsymbol{x})$, and so by symmetry of the inner product it follows that $\kappa(\boldsymbol{x}, \boldsymbol{x}') = \kappa(\boldsymbol{x}', \boldsymbol{x})$. As a consequence, reproducing kernels are necessarily *symmetric* functions. Moreover, a reproducing kernel κ is a *positive semidefinite* function, meaning that for every $n \geqslant 1$ and every choice of $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ and $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathcal{X}$, it holds that

REPRODUCING PROPERTY

POSITIVE SEMIDEFINITE

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) \, \alpha_j \geqslant 0. \tag{6.13}$$

In other words, *every* Gram matrix $\mathbf{K}$ associated with κ is a positive semidefinite matrix; that is $\boldsymbol{\alpha}^\top \mathbf{K} \boldsymbol{\alpha} \geqslant 0$ for all $\boldsymbol{\alpha}$. The proof is addressed in Exercise 1.

The following theorem gives an alternative characterization of an RKHS. The proof uses the Riesz representation Theorem A.17. Also note that in the theorem below we could have replaced the word "bounded" with "continuous", as the two are equivalent for linear functionals; see Theorem A.16.

☞ 392

Theorem 6.1: Continuous Evaluation Functionals Characterize a RKHS

An RKHS $\mathcal{G}$ on a set $\mathcal{X}$ is a Hilbert space in which every *evaluation functional* $\delta_{\boldsymbol{x}} : g \mapsto g(\boldsymbol{x})$ is bounded. Conversely, a Hilbert space $\mathcal{G}$ of functions $\mathcal{X} \to \mathbb{R}$ for which every evaluation functional is bounded is an RKHS.

EVALUATION FUNCTIONAL

Proof: Note that, since evaluation functionals $\delta_{\boldsymbol{x}}$ are linear operators, showing boundedness is equivalent to showing continuity. Given an RKHS with reproducing kernel κ, suppose that we have a sequence $g_n \in \mathcal{G}$ converging to $g \in \mathcal{G}$, that is $\|g_n - g\|_{\mathcal{G}} \to 0$. We apply the Cauchy–Schwarz inequality (Theorem A.15) and the reproducing property of κ to find that for every $\boldsymbol{x} \in \mathcal{X}$ and any n:

☞ 391

$$\begin{aligned} |\delta_{\boldsymbol{x}} g_n - \delta_{\boldsymbol{x}} g| &= |g_n(\boldsymbol{x}) - g(\boldsymbol{x})| = |\langle g_n - g, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}}| \leqslant \|g_n - g\|_{\mathcal{G}} \, \|\kappa_{\boldsymbol{x}}\|_{\mathcal{G}} = \|g_n - g\|_{\mathcal{G}} \sqrt{\langle \kappa_{\boldsymbol{x}}, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}}} \\ &= \|g_n - g\|_{\mathcal{G}} \sqrt{\kappa(\boldsymbol{x}, \boldsymbol{x})}. \end{aligned}$$

Noting that $\sqrt{\kappa(\boldsymbol{x}, \boldsymbol{x})} < \infty$ by definition for every $\boldsymbol{x} \in \mathcal{X}$, and that $\|g_n - g\|_{\mathcal{G}} \to 0$ as $n \to \infty$, we have shown continuity of $\delta_{\boldsymbol{x}}$, that is $|\delta_{\boldsymbol{x}} g_n - \delta_{\boldsymbol{x}} g| \to 0$ as $n \to \infty$ for every $\boldsymbol{x} \in \mathcal{X}$.

Conversely, suppose that evaluation functionals are bounded. Then from the Riesz representation Theorem A.17, there exists some $g_{\delta_x} \in \mathcal{G}$ such that $\delta_x g = \langle g, g_{\delta_x} \rangle_{\mathcal{G}}$ for all $g \in \mathcal{G}$ — the *representer* of evaluation. If we define $\kappa(\boldsymbol{x}, \boldsymbol{x}') = g_{\delta_x}(\boldsymbol{x}')$ for all $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}$, then $\kappa_{\boldsymbol{x}} := \kappa(\boldsymbol{x}, \cdot) = g_{\delta_x}$ is an element of $\mathcal{G}$ for every $\boldsymbol{x} \in \mathcal{X}$ and $\langle g, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}} = \delta_x g = g(\boldsymbol{x})$, so that the reproducing property in Definition 6.1 is verified. □

The fact that an RKHS has continuous evaluation functionals means that if two functions $g, h \in \mathcal{G}$ are "close" with respect to $\|\cdot\|_{\mathcal{G}}$, then their evaluations $g(\boldsymbol{x}), h(\boldsymbol{x})$ are close *for every* $\boldsymbol{x} \in \mathcal{X}$. Formally, convergence in $\|\cdot\|_{\mathcal{G}}$ norm implies pointwise convergence for all $\boldsymbol{x} \in \mathcal{X}$.

The following theorem shows that any finite function $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ can serve as a reproducing kernel as long as it is finite, symmetric, and positive semidefinite. The corresponding (unique!) RKHS $\mathcal{G}$ is the completion of the set of all functions of the form $\sum_{i=1}^{n} \alpha_i \kappa_{\boldsymbol{x}_i}$ where $\alpha_i \in \mathbb{R}$ for all $i = 1, \ldots, n$.

Theorem 6.2: Moore–Aronszajn

Given a non-empty set $\mathcal{X}$ and any finite symmetric positive semidefinite function $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, there exists an RKHS $\mathcal{G}$ of functions $g : \mathcal{X} \to \mathbb{R}$ with reproducing kernel κ. Moreover, $\mathcal{G}$ is unique.

Proof: (Sketch) As the proof of uniqueness is treated in Exercise 2, the objective is to prove existence. The idea is to construct a pre-RKHS $\mathcal{G}_0$ from the given function κ that has the essential structure and then to extend $\mathcal{G}_0$ to an RKHS $\mathcal{G}$.

In particular, define $\mathcal{G}_0$ as the set of finite linear combinations of functions $\kappa_{\boldsymbol{x}}$, $\boldsymbol{x} \in \mathcal{X}$:

$$\mathcal{G}_0 := \left\{ g = \sum_{i=1}^{n} \alpha_i \kappa_{\boldsymbol{x}_i} \;\middle|\; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathcal{X},\ \alpha_i \in \mathbb{R},\ n \in \mathbb{N} \right\}.$$

Define on $\mathcal{G}_0$ the following inner product:

$$\langle f, g \rangle_{\mathcal{G}_0} := \left\langle \sum_{i=1}^{n} \alpha_i \kappa_{\boldsymbol{x}_i}, \sum_{j=1}^{m} \beta_j \kappa_{\boldsymbol{x}'_j} \right\rangle_{\mathcal{G}_0} := \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i \beta_j \kappa(\boldsymbol{x}_i, \boldsymbol{x}'_j).$$

Then $\mathcal{G}_0$ is an inner product space. In fact, $\mathcal{G}_0$ has the essential structure we require, namely that (i) evaluation functionals are bounded/continuous (Exercise 4) and (ii) Cauchy sequences in $\mathcal{G}_0$ that converge pointwise also converge in norm (see Exercise 5).

We then enlarge $\mathcal{G}_0$ to the set $\mathcal{G}$ of all functions $g : \mathcal{X} \to \mathbb{R}$ for which there exists a Cauchy sequence in $\mathcal{G}_0$ converging pointwise to g and define an inner product on $\mathcal{G}$ as the limit

$$\langle f, g \rangle_{\mathcal{G}} := \lim_{n \to \infty} \langle f_n, g_n \rangle_{\mathcal{G}_0}, \tag{6.14}$$

where $f_n \to f$ and $g_n \to g$. To show that $\mathcal{G}$ is an RKHS it remains to be shown that (1) this inner product is well defined; (2) evaluation functionals remain bounded; and (3) the space $\mathcal{G}$ is complete. A detailed proof is established in Exercises 6 and 7. □

6.4 Construction of Reproducing Kernels

In this section we describe various ways to construct a reproducing kernel $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ for some feature space $\mathcal{X}$. Recall that κ needs to be a finite, symmetric, and positive semidefinite function (that is, it satisfies (6.13)). In view of Theorem 6.2, specifying the space $\mathcal{X}$ and a reproducing kernel $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ corresponds to *uniquely* specifying an RKHS.

6.4.1 Reproducing Kernels via Feature Mapping

Perhaps the most fundamental way to construct a reproducing kernel κ is via a feature map $\boldsymbol{\phi} : \mathcal{X} \to \mathbb{R}^p$. We define $\kappa(\boldsymbol{x}, \boldsymbol{x}') := \langle \boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}') \rangle$, where $\langle\ ,\ \rangle$ denotes the Euclidean inner product. The function is clearly finite and symmetric. To verify that κ is positive semidefinite, let $\boldsymbol{\Phi}$ be the matrix with rows $\boldsymbol{\phi}(\boldsymbol{x}_1)^\top, \ldots, \boldsymbol{\phi}(\boldsymbol{x}_n)^\top$ and let $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_n]^\top \in \mathbb{R}^n$. Then,

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) \, \alpha_j = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \, \boldsymbol{\phi}^\top(\boldsymbol{x}_i) \, \boldsymbol{\phi}(\boldsymbol{x}_j) \, \alpha_j = \boldsymbol{\alpha}^\top \boldsymbol{\Phi} \boldsymbol{\Phi}^\top \boldsymbol{\alpha} = \|\boldsymbol{\Phi}^\top \boldsymbol{\alpha}\|^2 \geqslant 0.$$

■ **Example 6.4 (Linear Kernel)** Taking the identity feature map $\boldsymbol{\phi}(\boldsymbol{x}) = \boldsymbol{x}$ on $\mathcal{X} = \mathbb{R}^p$, gives the *linear kernel* LINEAR KERNEL

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = \langle \boldsymbol{x}, \boldsymbol{x}' \rangle = \boldsymbol{x}^\top \boldsymbol{x}'.$$

As can be seen from the proof of Theorem 6.2, the RKHS of functions corresponding to the linear kernel is the space of *linear* functions on $\mathbb{R}^p$. This space is isomorphic to $\mathbb{R}^p$ itself, as discussed in the introduction (see also Exercise 12). ■

It is natural to wonder whether a given kernel function corresponds uniquely to a feature map. The answer is no, as we shall see by way of example.

■ **Example 6.5 (Feature Maps and Kernel Functions)** Let $\mathcal{X} = \mathbb{R}$ and consider feature maps $\phi_1 : \mathcal{X} \to \mathbb{R}$ and $\boldsymbol{\phi}_2 : \mathcal{X} \to \mathbb{R}^2$, with $\phi_1(x) := x$ and $\boldsymbol{\phi}_2(x) := [x, x]^\top / \sqrt{2}$. Then

$$\kappa_{\phi_1}(x, x') = \langle \phi_1(x), \phi_1(x') \rangle = x x',$$

but also

$$\kappa_{\boldsymbol{\phi}_2}(x, x') = \langle \boldsymbol{\phi}_2(x), \boldsymbol{\phi}_2(x') \rangle = x x'.$$

Thus, we arrive at the same kernel function defined for the same underlying set $\mathcal{X}$ via two different feature maps. ■

6.4.2 Kernels from Characteristic Functions

Another way to construct reproducing kernels on $\mathcal{X} = \mathbb{R}^p$ makes use of the properties of *characteristic functions*. In particular, we have the following result. We leave its proof as Exercise 10. ☞ 443

Theorem 6.3: Reproducing Kernel from a Characteristic Function

Let $\boldsymbol{X} \sim \mu$ be an $\mathbb{R}^p$-valued random vector that is symmetric about the origin (that is, $\boldsymbol{X}$ and $-\boldsymbol{X}$ are identically distributed), and let ψ be its characteristic function: $\psi(\boldsymbol{t}) = \mathbb{E}\, \mathrm{e}^{\mathrm{i}\boldsymbol{t}^\top \boldsymbol{X}} = \int \mathrm{e}^{\mathrm{i}\boldsymbol{t}^\top \boldsymbol{x}}\, \mu(\mathrm{d}\boldsymbol{x})$ for $\boldsymbol{t} \in \mathbb{R}^p$. Then $\kappa(\boldsymbol{x}, \boldsymbol{x}') := \psi(\boldsymbol{x} - \boldsymbol{x}')$ is a valid reproducing kernel on $\mathbb{R}^p$.

■ **Example 6.6 (Gaussian Kernel)** The multivariate normal distribution with mean vector $\mathbf{0}$ and covariance matrix $b^2\, \mathbf{I}_p$ is clearly symmetric around the origin. Its characteristic function is

$$\psi(\boldsymbol{t}) = \exp\left(-\frac{1}{2} b^2\, \|\boldsymbol{t}\|^2\right), \quad \boldsymbol{t} \in \mathbb{R}^p.$$

GAUSSIAN KERNEL

Taking $b^2 = 1/\sigma^2$, this gives the popular *Gaussian kernel* on $\mathbb{R}^p$:

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = \exp\left(-\frac{1}{2} \frac{\|\boldsymbol{x} - \boldsymbol{x}'\|^2}{\sigma^2}\right). \tag{6.15}$$

BANDWIDTH

The parameter σ is sometimes called the *bandwidth*. Note that in the machine learning literature, the Gaussian kernel is sometimes referred to as "the" *radial basis function (rbf) kernel*.[1]

RADIAL BASIS FUNCTION (RBF) KERNEL

From the proof of Theorem 6.2, we see that the RKHS $\mathcal{G}$ determined by the Gaussian kernel κ is the space of pointwise limits of functions of the form

$$g(\boldsymbol{x}) = \sum_{i=1}^{n} \alpha_i \exp\left(-\frac{1}{2} \frac{\|\boldsymbol{x} - \boldsymbol{x}_i\|^2}{\sigma^2}\right).$$

We can think of each point $\boldsymbol{x}_i$ having a feature $\kappa_{\boldsymbol{x}_i}$ that is a scaled multivariate Gaussian pdf centered at $\boldsymbol{x}_i$. ■

■ **Example 6.7 (Sinc Kernel)** The characteristic function of a $\mathsf{Uniform}[-1, 1]$ random variable (which is symmetric around 0) is $\psi(t) = \mathrm{sinc}(t) := \sin(t)/t$, so $\kappa(x, x') = \mathrm{sinc}(x - x')$ is a valid kernel. ■

☞ 131

Inspired by kernel density estimation (Section 4.4), we may be tempted to use the pdf of a random variable that is symmetric about the origin to construct a reproducing kernel. However, doing so will not work in general, as the next example illustrates.

■ **Example 6.8 (Uniform pdf Does not Construct a Valid Reproducing Kernel)** Take the function $\psi(t) = \frac{1}{2}\mathbb{1}\{|t| \leqslant 1\}$, which is the pdf of $X \sim \mathsf{Uniform}[-1, 1]$. Unfortunately, the function $\kappa(x, x') = \psi(x - x')$ is not positive semidefinite, as can be seen for example by constructing the matrix $\mathbf{A} = [\kappa(t_i, t_j), i, j = 1, 2, 3]$ for the points $t_1 = 0$, $t_2 = 0.75$, and $t_3 = 1.5$ as follows:

$$\mathbf{A} = \begin{pmatrix} \psi(0) & \psi(-0.75) & \psi(-1.5) \\ \psi(0.75) & \psi(0) & \psi(-0.75) \\ \psi(1.5) & \psi(0.75) & \psi(0) \end{pmatrix} = \begin{pmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.5 & 0.5 \\ 0 & 0.5 & 0.5 \end{pmatrix}.$$

The eigenvalues of $\mathbf{A}$ are $\{1/2 - \sqrt{1/2}, 1/2, 1/2 + \sqrt{1/2}\} \approx \{-0.2071, 0.5, 1.2071\}$ and so by Theorem A.9, $\mathbf{A}$ is not a positive semidefinite matrix, since it has a negative eigenvalue. Consequently, κ is not a valid reproducing kernel. ■

☞ 369

One of the reasons why the Gaussian kernel (6.15) is popular is that it enjoys the *universal approximation property* [88]: the space of functions spanned by the Gaussian kernel is dense in the space of continuous functions with support $\mathcal{Z} \subset \mathbb{R}^p$. Naturally, this is a desirable property especially if there is little prior knowledge about the properties of g^*. However, note that *every* function g in the RKHS $\mathcal{G}$ associated with a Gaussian kernel κ is infinitely differentiable. Moreover, a Gaussian RKHS does not contain non-zero constant functions. Indeed, if $A \subset \mathcal{Z}$ is non-empty and open, then the only function of the form $g(\boldsymbol{x}) = c\,\mathbb{1}\{\boldsymbol{x} \in A\}$ contained in $\mathcal{G}$ is the zero function ($c = 0$).

UNIVERSAL APPROXIMATION PROPERTY

Consequently, if it is known that g is differentiable only to a certain order, one may prefer the *Matérn kernel* with parameters $\nu, \sigma > 0$:

MATÉRN KERNEL

$$\kappa_\nu(\boldsymbol{x}, \boldsymbol{x}') = \frac{2^{1-\nu}}{\Gamma(\nu)} \left(\sqrt{2\nu}\,\|\boldsymbol{x} - \boldsymbol{x}'\|/\sigma\right)^\nu K_\nu\left(\sqrt{2\nu}\,\|\boldsymbol{x} - \boldsymbol{x}'\|/\sigma\right), \tag{6.16}$$

which gives functions that are (weakly) differentiable to order $\lfloor \nu \rfloor$ (but not necessarily to order $\lceil \nu \rceil$). Here, K_ν denotes the modified Bessel function of the second kind; see (4.49). The particular form of the Matérn kernel appearing in (6.16) ensures that $\lim_{\nu\to\infty} \kappa_\nu(\boldsymbol{x}, \boldsymbol{x}') = \kappa(\boldsymbol{x}, \boldsymbol{x}')$, where κ is the Gaussian kernel appearing in (6.15).

☞ 163

We remark that Sobolev spaces are closely related to the Matérn kernel. Up to constants (which scale the unit ball in the space), in dimension p and for a parameter $s > p/2$, these spaces can be identified with $\psi(\boldsymbol{t}) = \frac{2^{1-s}}{\Gamma(s)} \|\boldsymbol{t}\|^{s-p/2} K_{p/2-s}(\|\boldsymbol{t}\|)$, which in turn can be viewed as the characteristic function corresponding to the (radially symmetric) multivariate Student's t distribution with s degrees of freedom: that is, with pdf $f(\boldsymbol{x}) \propto (1 + \|\boldsymbol{x}\|^2)^{-s}$.

☞ 162

6.4.3 Reproducing Kernels Using Orthonormal Features

We have seen in Sections 6.4.1 and 6.4.2 how to construct reproducing kernels from feature maps and characteristic functions. Another way to construct kernels on a space $\mathcal{X}$ is to work directly from the function class $L^2(\mathcal{X}; \mu)$; that is, the set of square-integrable[2] functions on $\mathcal{X}$ with respect to μ; see also Definition A.4. For simplicity, in what follows, we will consider μ to be the Lebesgue measure, and will simply write $L^2(\mathcal{X})$ rather than $L^2(\mathcal{X}; \mu)$. We will also assume that $\mathcal{X} \subseteq \mathbb{R}^p$.

☞ 387

Let $\{\xi_1, \xi_2, \ldots\}$ be an orthonormal basis of $L^2(\mathcal{X})$ and let $c_1, c_2, \ldots$ be a sequence of positive numbers. As discussed in Section 6.4.1, the kernel corresponding to a feature map $\boldsymbol{\phi} : \mathcal{X} \to \mathbb{R}^p$ is $\kappa(\boldsymbol{x}, \boldsymbol{x}') = \boldsymbol{\phi}(\boldsymbol{x})^\top \boldsymbol{\phi}(\boldsymbol{x}') = \sum_{i=1}^p \phi_i(\boldsymbol{x})\,\phi_i(\boldsymbol{x}')$. Now consider a (possibly infinite) sequence of feature functions $\phi_i = c_i\,\xi_i$, $i = 1, 2, \ldots$ and define

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') := \sum_{i\geqslant 1} \phi_i(\boldsymbol{x})\,\phi_i(\boldsymbol{x}') = \sum_{i\geqslant 1} \lambda_i\,\xi_i(\boldsymbol{x})\,\xi_i(\boldsymbol{x}'), \tag{6.17}$$

[1] The term radial basis function is sometimes used more generally to mean kernels of the form $\kappa(\boldsymbol{x}, \boldsymbol{x}') = f(\|\boldsymbol{x} - \boldsymbol{x}'\|)$ for some function $f : \mathbb{R} \to \mathbb{R}$.

[2] A function $f : \mathcal{X} \to \mathbb{R}$ is said to be square-integrable if $\int f^2(\boldsymbol{x})\,\mu(\mathrm{d}\boldsymbol{x}) < \infty$, where μ is a measure on $\mathcal{X}$.

where $\lambda_i = c_i^2, i = 1, 2, \ldots$. This is well-defined as long as $\sum_{i\geqslant 1} \lambda_i < \infty$, which we assume from now on. Let $\mathcal{H}$ be the linear space of functions of the form $f = \sum_{i\geqslant 1} \alpha_i \xi_i$, where $\sum_{i\geqslant 1} \alpha_i^2/\lambda_i < \infty$. As every function $f \in L^2(\mathcal{X})$ can be represented as $f = \sum_{i\geqslant 1} \langle f, \xi_i\rangle \xi_i$, we see that $\mathcal{H}$ is a linear subspace of $L^2(\mathcal{X})$. On $\mathcal{H}$ define the inner product

$$\langle f, g\rangle_{\mathcal{H}} := \sum_{i\geqslant 1} \frac{\langle f, \xi_i\rangle\langle g, \xi_i\rangle}{\lambda_i}.$$

With this inner product, the squared norm of $f = \sum_{i\geqslant 1} \alpha_i \xi_i$ is $\|f\|_{\mathcal{H}}^2 = \sum_{i\geqslant 1} \alpha_i^2/\lambda_i < \infty$. We show that $\mathcal{H}$ is actually an RKHS with kernel κ by verifying the conditions of Definition 6.1. First,

$$\kappa_{\boldsymbol{x}} = \sum_{i\geqslant 1} \lambda_i \xi_i(\boldsymbol{x})\, \xi_i \in \mathcal{H},$$

as $\sum_i \lambda_i < \infty$ by assumption, and so κ is finite. Second, the reproducing property holds. Namely, let $f = \sum_{i\geqslant 1} \alpha_i \xi_i$. Then,

$$\langle \kappa_{\boldsymbol{x}}, f\rangle_{\mathcal{H}} = \sum_{i\geqslant 1} \frac{\langle \kappa_{\boldsymbol{x}}, \xi_i\rangle\langle f, \xi_i\rangle}{\lambda_i} = \sum_{i\geqslant 1} \frac{\lambda_i \xi_i(\boldsymbol{x})\, \alpha_i}{\lambda_i} = \sum_{i\geqslant 1} \alpha_i \xi_i(\boldsymbol{x}) = f(\boldsymbol{x}).$$

The discussion above demonstrates that kernels can be constructed via (6.17). In fact, (under mild conditions) any given reproducing kernel κ can be written in the form (6.17), where this series representation enjoys desirable convergence properties. This result is known as Mercer's theorem, and is given below. We leave the full proof including the precise conditions to, e.g., [40], but the main idea is that a reproducing kernel κ can be thought of as a generalization of a positive semidefinite matrix $\mathbf{K}$, and can also be written in spectral form (see also Section A.6.5). In particular, by Theorem A.9, we can write $\mathbf{K} = \mathbf{V}\mathbf{D}\mathbf{V}^\top$, where $\mathbf{V}$ is a matrix of orthonormal eigenvectors $[\boldsymbol{v}_\ell]$ and $\mathbf{D}$ the diagonal matrix of the (positive) eigenvalues $[\lambda_\ell]$; that is,

☞ 369

$$\mathbf{K}(i, j) = \sum_{\ell\geqslant 1} \lambda_\ell\, v_\ell(i)\, v_\ell(j).$$

In (6.18) below, $\boldsymbol{x}, \boldsymbol{x}'$ play the role of i, j, and ξ_ℓ plays the role of $\boldsymbol{v}_\ell$.

Theorem 6.4: Mercer

Let $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ be a reproducing kernel for a compact set $\mathcal{X} \subset \mathbb{R}^p$. Then (under mild conditions) there exists a countable sequence of non-negative numbers $\{\lambda_\ell\}$ decreasing to zero and functions $\{\xi_\ell\}$ orthonormal in $L^2(\mathcal{X})$ such that

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = \sum_{\ell\geqslant 1} \lambda_\ell\, \xi_\ell(\boldsymbol{x})\, \xi_\ell(\boldsymbol{x}'), \qquad \text{for all } \boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}, \tag{6.18}$$

where (6.18) converges absolutely and uniformly on $\mathcal{X} \times \mathcal{X}$.

Further, if $\lambda_\ell > 0$, then (λ_ℓ, ξ_ℓ) is an (eigenvalue, eigenfunction) pair for the integral operator $K : L^2(\mathcal{X}) \to L^2(\mathcal{X})$ defined by $[Kf](\boldsymbol{x}) := \int_{\mathcal{X}} \kappa(\boldsymbol{x}, \boldsymbol{y}) f(\boldsymbol{y})\, \mathrm{d}\boldsymbol{y}$ for $\boldsymbol{x} \in \mathcal{X}$.

Theorem 6.4 holds if (i) the kernel κ is continuous on $\mathcal{X} \times \mathcal{X}$, (ii) the function $\widetilde{\kappa}(\boldsymbol{x}) := \kappa(\boldsymbol{x}, \boldsymbol{x})$ defined for $\boldsymbol{x} \in \mathcal{X}$ is integrable. Extensions of Theorem 6.4 to more general spaces $\mathcal{X}$ and measures μ hold; see, e.g., [115] or [40].

The key importance of Theorem 6.4 lies in the fact that the series representation (6.18) converges absolutely and uniformly on $\mathcal{X} \times \mathcal{X}$. The uniform convergence is a much stronger condition than pointwise convergence, and means for instance that properties of the sequence of partial sums, such as continuity and integrability, are transferred to the limit.

■ **Example 6.9 (Mercer)** Suppose $\mathcal{X} = [-1, 1]$ and the kernel is $\kappa(x, x') = 1 + xx'$ which corresponds to the RKHS $\mathcal{G}$ of affine functions from $\mathcal{X} \to \mathbb{R}$. To find the (eigenvalue, eigenfunction) pairs for the integral operator appearing in Theorem 6.4, we need to find numbers $\{\lambda_\ell\}$ and orthonormal functions $\{\xi_\ell(x)\}$ that solve

$$\int_{-1}^{1} (1 + xx')\, \xi_\ell(x')\, \mathrm{d}x' = \lambda_\ell\, \xi_\ell(x), \quad \text{for all } x \in [-1, 1].$$

Consider first a constant function $\xi_1(x) = c$. Then, for all $x \in [-1, 1]$, we have that $2c = \lambda_1 c$, and the normalization condition requires that $\int_{-1}^{1} c^2\, \mathrm{d}x = 1$. Together, these give $\lambda_1 = 2$ and $c = \pm 1/\sqrt{2}$. Next, consider an affine function $\xi_2(x) = a + bx$. Orthogonality requires that

$$\int_{-1}^{1} c(a + bx)\, \mathrm{d}x = 0,$$

which implies $a = 0$ (since $c \neq 0$). Moreover, the normalization condition then requires

$$\int_{-1}^{1} b^2 x^2\, \mathrm{d}x = 1,$$

or, equivalently, $2b^2/3 = 1$, implying $b = \pm\sqrt{3/2}$. Finally, the integral equation reads

$$\int_{-1}^{1} (1 + xx')\, bx'\, \mathrm{d}x' = \lambda_2\, bx \iff \frac{2bx}{3} = \lambda_2 bx,$$

implying that $\lambda_2 = 2/3$. We take the positive solutions (i.e., $c > 0$ and $b > 0$), and note that

$$\lambda_1\, \xi_1(x)\, \xi_1(x') + \lambda_2\, \xi_2(x)\, \xi_2(x') = 2\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} + \frac{2}{3}\frac{\sqrt{3}}{\sqrt{2}}x\frac{\sqrt{3}}{\sqrt{2}}x' = 1 + xx' = \kappa(x, x'),$$

and so we have found the decomposition appearing in (6.18). As an aside, observe that ξ_1 and ξ_2 are orthonormal versions of the first two Legendre polynomials. The corresponding feature map can be explicitly identified as $\phi_1(x) = \sqrt{\lambda_1}\, \xi_1(x) = 1$ and $\phi_2(x) = \sqrt{\lambda_2}\, \xi_2(x) = x$. ■

☞ 389

6.4.4 Kernels from Kernels

The following theorem lists some useful properties for constructing reproducing kernels from existing reproducing kernels.

Theorem 6.5: Rules for Constructing Kernels from Other Kernels

1. If $\kappa : \mathbb{R}^p \times \mathbb{R}^p \to \mathbb{R}$ is a reproducing kernel and $\boldsymbol{\phi} : \mathcal{X} \to \mathbb{R}^p$ is a function, then $\kappa(\boldsymbol{\phi}(\boldsymbol{x}), \boldsymbol{\phi}(\boldsymbol{x}'))$ is a reproducing kernel from $\mathcal{X} \times \mathcal{X} \to \mathbb{R}$.
2. If $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ is a reproducing kernel and $f : \mathcal{X} \to \mathbb{R}_+$ is a function, then $f(\boldsymbol{x})\kappa(\boldsymbol{x}, \boldsymbol{x}')f(\boldsymbol{x}')$ is also a reproducing kernel from $\mathcal{X} \times \mathcal{X} \to \mathbb{R}$.
3. If κ_1 and κ_2 are reproducing kernels from $\mathcal{X} \times \mathcal{X} \to \mathbb{R}$, then so is their sum $\kappa_1 + \kappa_2$.
4. If κ_1 and κ_2 are reproducing kernels from $\mathcal{X} \times \mathcal{X} \to \mathbb{R}$, then so is their product $\kappa_1\kappa_2$.
5. If κ_1 and κ_2 are reproducing kernels from $\mathcal{X} \times \mathcal{X} \to \mathbb{R}$ and $\mathcal{Y} \times \mathcal{Y} \to \mathbb{R}$ respectively, then $\kappa_+((\boldsymbol{x}, \boldsymbol{y}), (\boldsymbol{x}', \boldsymbol{y}')) := \kappa_1(\boldsymbol{x}, \boldsymbol{x}') + \kappa_2(\boldsymbol{y}, \boldsymbol{y}')$ and $\kappa_\times((\boldsymbol{x}, \boldsymbol{y}), (\boldsymbol{x}', \boldsymbol{y}')) := \kappa_1(\boldsymbol{x}, \boldsymbol{x}')\kappa_2(\boldsymbol{y}, \boldsymbol{y}')$ are reproducing kernels from $(\mathcal{X} \times \mathcal{Y}) \times (\mathcal{X} \times \mathcal{Y}) \to \mathbb{R}$.

Proof: For Rules 1, 2, and 3 it is easy to verify that the resulting function is finite, symmetric, and positive semidefinite, and so is a valid reproducing kernel by Theorem 6.2. For example, for Rule 1 we have $\sum_{i=1}^n \sum_{j=1}^n \alpha_i \kappa(\boldsymbol{y}_i, \boldsymbol{y}_j)\alpha_j \geqslant 0$ for every choice of $\{\alpha_i\}_{i=1}^n$ and $\{\boldsymbol{y}_i\}_{i=1}^n \in \mathbb{R}^p$, since κ is a reproducing kernel. In particular, it holds true for $\boldsymbol{y}_i = \boldsymbol{\phi}(\boldsymbol{x}_i)$, $i = 1, \ldots, n$. Rule 4 is easy to show for kernels κ_1, κ_2 that admit a representation of the form (6.17), since

$$\begin{aligned}
\kappa_1(\boldsymbol{x}, \boldsymbol{x}')\,\kappa_2(\boldsymbol{x}, \boldsymbol{x}') &= \left(\sum_{i \geqslant 1} \phi_i^{(1)}(\boldsymbol{x})\,\phi_i^{(1)}(\boldsymbol{x}')\right)\left(\sum_{j \geqslant 1} \phi_j^{(2)}(\boldsymbol{x})\,\phi_j^{(2)}(\boldsymbol{x}')\right) \\
&= \sum_{i,j \geqslant 1} \phi_i^{(1)}(\boldsymbol{x})\,\phi_j^{(2)}(\boldsymbol{x})\,\phi_i^{(1)}(\boldsymbol{x}')\,\phi_j^{(2)}(\boldsymbol{x}') \\
&= \sum_{k \geqslant 1} \phi_k(\boldsymbol{x})\,\phi_k(\boldsymbol{x}') =: \kappa(\boldsymbol{x}, \boldsymbol{x}'),
\end{aligned}$$

showing that $\kappa = \kappa_1\kappa_2$ also admits a representation of the form (6.17), where the new (possibly infinite) sequence of features (ϕ_k) is identified in a one-to-one way with the sequence $(\phi_i^{(1)}\phi_j^{(2)})$. We leave the proof of rule 5 as an exercise (Exercise 8). □

■ **Example 6.10 (Polynomial Kernel)** Consider $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{R}^2$ with

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = (1 + \langle \boldsymbol{x}, \boldsymbol{x}' \rangle)^2,$$

POLYNOMIAL KERNEL

where $\langle \boldsymbol{x}, \boldsymbol{x}' \rangle = \boldsymbol{x}^\top \boldsymbol{x}'$. This is an example of a *polynomial kernel*. Combining the fact that sums and products of kernels are again kernels (rules 3 and 4 of Theorem 6.5), we find that, since $\langle \boldsymbol{x}, \boldsymbol{x}' \rangle$ and the constant function 1 are kernels, so are $1 + \langle \boldsymbol{x}, \boldsymbol{x}' \rangle$ and $(1 + \langle \boldsymbol{x}, \boldsymbol{x}' \rangle)^2$. By writing

$$\begin{aligned}
\kappa(\boldsymbol{x}, \boldsymbol{x}') &= (1 + x_1 x_1' + x_2 x_2')^2 \\
&= 1 + 2x_1 x_1' + 2x_2 x_2' + 2x_1 x_2 x_1' x_2' + (x_1 x_1')^2 + (x_2 x_2')^2,
\end{aligned}$$

we see that $\kappa(\boldsymbol{x}, \boldsymbol{x}')$ can be written as the inner product in $\mathbb{R}^6$ of the two feature vectors $\boldsymbol{\phi}(\boldsymbol{x})$ and $\boldsymbol{\phi}(\boldsymbol{x}')$, where the feature map $\boldsymbol{\phi} : \mathbb{R}^2 \to \mathbb{R}^6$ can be explicitly identified as

$$\boldsymbol{\phi}(\boldsymbol{x}) = [1,\ \sqrt{2}x_1,\ \sqrt{2}x_2,\ \sqrt{2}x_1x_2, x_1^2, x_2^2]^\top.$$

Thus, the RKHS determined by κ can be explicitly identified with the space of functions $\boldsymbol{x} \mapsto \boldsymbol{\phi}(\boldsymbol{x})^\top\boldsymbol{\beta}$ for some $\boldsymbol{\beta} \in \mathbb{R}^6$. ■

In the above example we could explicitly identify the feature map. However, in general a feature map need not be explicitly available. Using a particular reproducing kernel corresponds to using an *implicit* (possibly infinite dimensional!) feature map that never needs to be explicitly computed.

6.5 Representer Theorem

Recall the setting discussed at the beginning of this chapter: we are given training data $\tau = \{(\boldsymbol{x}_i, y_i)\}_{i=1}^n$ and a loss function that measures the fit to the data, and we wish to find a function g that minimizes the training loss, with the addition of a regularization term, as described in Section 6.2. To do this, we assume first that the class $\mathcal{G}$ of prediction functions can be decomposed as the direct sum of an RKHS $\mathcal{H}$, defined by a kernel function $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, and another linear space of real-valued functions $\mathcal{H}_0$ on $\mathcal{X}$; that is,

$$\mathcal{G} = \mathcal{H} \oplus \mathcal{H}_0,$$

meaning that any element $g \in \mathcal{G}$ can be written as $g = h + h_0$, with $h \in \mathcal{H}$ and $h_0 \in \mathcal{H}_0$. In minimizing the training loss we wish to penalize the h term of g but not the h_0 term. Specifically, the aim is to solve the functional optimization problem

$$\min_{g \in \mathcal{H} \oplus \mathcal{H}_0} \frac{1}{n} \sum_{i=1}^n \text{Loss}(y_i, g(\boldsymbol{x}_i)) + \gamma \|g\|_{\mathcal{H}}^2. \tag{6.19}$$

Here, we use a slight abuse of notation: $\|g\|_{\mathcal{H}}$ means $\|h\|_{\mathcal{H}}$ if $g = h + h_0$, as above. In this way, we can view $\mathcal{H}_0$ as the null space of the functional $g \mapsto \|g\|_{\mathcal{H}}$. This null space may be empty, but typically has a small dimension m; for example it could be the one-dimensional space of constant functions, as in Example 6.2. ☞ 217

■ **Example 6.11 (Null Space)** Consider again the setting of Example 6.2, for which we have feature vectors $\widetilde{\boldsymbol{x}} = [1, \boldsymbol{x}^\top]^\top$ and $\mathcal{G}$ consists of functions of the form $g : \widetilde{\boldsymbol{x}} \mapsto \beta_0 + \boldsymbol{x}^\top\boldsymbol{\beta}$. Each function g can be decomposed as $g = h + h_0$, where $h : \widetilde{\boldsymbol{x}} \mapsto \boldsymbol{x}^\top\boldsymbol{\beta}$, and $h_0 : \widetilde{\boldsymbol{x}} \mapsto \beta_0$.

Given $g \in \mathcal{G}$, we have $\|g\|_{\mathcal{H}} = \|\boldsymbol{\beta}\|$, and so the null space $\mathcal{H}_0$ of the functional $g \mapsto \|g\|_{\mathcal{H}}$ (that is, the set of all functions $g \in \mathcal{G}$ for which $\|g\|_{\mathcal{H}} = 0$) is the set of constant functions here, which has dimension $m = 1$. ■

Regularization favors elements in $\mathcal{H}_0$ and penalizes large elements in $\mathcal{H}$. As the regularization parameter γ varies between zero and infinity, solutions to (6.19) vary from "complex" ($g \in \mathcal{H} \oplus \mathcal{H}_0$) to "simple" ($g \in \mathcal{H}_0$).

A key reason why RKHSs are so useful is the following. By choosing $\mathcal{H}$ to be an RKHS in (6.19) this *functional* optimization problem effectively becomes a *parametric*

optimization problem. The reason is that any solution to (6.19) can be represented as a finite-dimensional linear combination of kernel functions, evaluated at the training sample. This is known as the *kernel trick*.

KERNEL TRICK

Theorem 6.6: Representer Theorem

The solution to the penalized optimization problem (6.19) is of the form

$$g(\boldsymbol{x}) = \sum_{i=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}) + \sum_{j=1}^{m} \eta_j \, q_j(\boldsymbol{x}), \tag{6.20}$$

where $\{q_1, \ldots, q_m\}$ is a basis of $\mathcal{H}_0$.

Proof: Let $\mathcal{F} = \text{Span}\,\{\kappa_{\boldsymbol{x}_i}, i = 1, \ldots, n\}$. Clearly, $\mathcal{F} \subseteq \mathcal{H}$. Then, the Hilbert space $\mathcal{H}$ can be represented as $\mathcal{H} = \mathcal{F} \oplus \mathcal{F}^\perp$, where $\mathcal{F}^\perp$ is the orthogonal complement of $\mathcal{F}$. In other words, $\mathcal{F}^\perp$ is the class of functions

$$\{f^\perp \in \mathcal{H} : \langle f^\perp, f \rangle_{\mathcal{H}} = 0, \;\; f \in \mathcal{F}\} \equiv \{f^\perp : \langle f^\perp, \kappa_{\boldsymbol{x}_i} \rangle_{\mathcal{H}} = 0, \;\; \forall i\}.$$

It follows, by the reproducing kernel property, that for all $f^\perp \in \mathcal{F}^\perp$:

$$f^\perp(\boldsymbol{x}_i) = \langle f^\perp, \kappa_{\boldsymbol{x}_i} \rangle_{\mathcal{H}} = 0, \quad i = 1, \ldots, n.$$

Now, take any $g \in \mathcal{H} \oplus \mathcal{H}_0$, and write it as $g = f + f^\perp + h_0$, with $f \in \mathcal{F}$, $f^\perp \in \mathcal{F}^\perp$, and $h_0 \in \mathcal{H}_0$. By the definition of the null space $\mathcal{H}_0$, we have $\|g\|^2_{\mathcal{H}} = \|f + f^\perp\|^2_{\mathcal{H}}$. Moreover, by Pythagoras' theorem, the latter is equal to $\|f\|^2_{\mathcal{H}} + \|f^\perp\|^2_{\mathcal{H}}$. It follows that

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^{n} \text{Loss}(y_i, g(\boldsymbol{x}_i)) + \gamma \|g\|^2_{\mathcal{H}} &= \frac{1}{n} \sum_{i=1}^{n} \text{Loss}(y_i, f(\boldsymbol{x}_i) + h_0(\boldsymbol{x}_i)) + \gamma \left(\|f\|^2_{\mathcal{H}} + \|f^\perp\|^2_{\mathcal{H}} \right) \\ &\geqslant \frac{1}{n} \sum_{i=1}^{n} \text{Loss}(y_i, f(\boldsymbol{x}_i) + h_0(\boldsymbol{x}_i)) + \gamma \, \|f\|^2_{\mathcal{H}}. \end{aligned}$$

Since we can obtain equality by taking $f^\perp = 0$, this implies that the minimizer of the penalized optimization problem (6.19) lies in the subspace $\mathcal{F} \oplus \mathcal{H}_0$ of $\mathcal{G} = \mathcal{H} \oplus \mathcal{H}_0$, and hence is of the form (6.20). □

Substituting the representation (6.20) of g into (6.19) gives the finite-dimensional optimization problem:

$$\min_{\boldsymbol{\alpha} \in \mathbb{R}^n, \, \boldsymbol{\eta} \in \mathbb{R}^m} \frac{1}{n} \sum_{i=1}^{n} \text{Loss}(y_i, (\mathbf{K}\boldsymbol{\alpha} + \mathbf{Q}\boldsymbol{\eta})_i) + \gamma \, \boldsymbol{\alpha}^\top \mathbf{K} \boldsymbol{\alpha}, \tag{6.21}$$

where

- $\mathbf{K}$ is the $n \times n$ (Gram) matrix with entries $[\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j), i = 1, \ldots, n, \;\; j = 1, \ldots, n]$.
- $\mathbf{Q}$ is the $n \times m$ matrix with entries $[q_j(\boldsymbol{x}_i), i = 1, \ldots, n, \;\; j = 1, \ldots, m]$.

In particular, for the squared-error loss we have

$$\min_{\boldsymbol{\alpha}\in\mathbb{R}^n,\,\boldsymbol{\eta}\in\mathbb{R}^m} \frac{1}{n}\left\|\boldsymbol{y}-(\mathbf{K}\boldsymbol{\alpha}+\mathbf{Q}\boldsymbol{\eta})\right\|^2+\gamma\,\boldsymbol{\alpha}^\top\mathbf{K}\boldsymbol{\alpha}. \tag{6.22}$$

This is a convex optimization problem, and its solution is found by differentiating (6.22) with respect to $\boldsymbol{\alpha}$ and $\boldsymbol{\eta}$ and equating to zero, leading to the following system of $(n+m)$ linear equations:

$$\begin{bmatrix}\mathbf{K}\mathbf{K}^\top+n\gamma\mathbf{K} & \mathbf{K}\mathbf{Q}\\ \mathbf{Q}^\top\mathbf{K}^\top & \mathbf{Q}^\top\mathbf{Q}\end{bmatrix}\begin{bmatrix}\boldsymbol{\alpha}\\ \boldsymbol{\eta}\end{bmatrix}=\begin{bmatrix}\mathbf{K}^\top\\ \mathbf{Q}^\top\end{bmatrix}\boldsymbol{y}. \tag{6.23}$$

As long as $\mathbf{Q}$ is of full column rank, the minimizing function is unique.

■ **Example 6.12 (Ridge Regression (cont.))** We return to Example 6.2 and identify that $\mathcal{H}$ is the RKHS with linear kernel function $\kappa(\boldsymbol{x},\boldsymbol{x}')=\boldsymbol{x}^\top\boldsymbol{x}'$ and $C=\mathcal{H}_0$ is the linear space of constant functions. In this case, $\mathcal{H}_0$ is spanned by the function $q_1\equiv 1$. Moreover, $\mathbf{K}=\mathbf{X}\mathbf{X}^\top$ and $\mathbf{Q}=\mathbf{1}$.

If we appeal to the representer theorem directly, then the problem in (6.6) becomes, as a result of (6.21):

$$\min_{\boldsymbol{\alpha},\eta_0}\frac{1}{n}\left\|\boldsymbol{y}-\eta_0\,\mathbf{1}-\mathbf{X}\mathbf{X}^\top\boldsymbol{\alpha}\right\|^2+\gamma\,\|\mathbf{X}^\top\boldsymbol{\alpha}\|^2.$$

This is a convex optimization problem, and so the solution follows by taking derivatives and setting them to zero. This gives the equations

$$\mathbf{X}\mathbf{X}^\top((\mathbf{X}\mathbf{X}^\top+n\gamma\,\mathbf{I}_n)\,\boldsymbol{\alpha}+\eta_0\,\mathbf{1}-\boldsymbol{y})=0,$$

and

$$n\,\eta_0=\mathbf{1}^\top(\boldsymbol{y}-\mathbf{X}\mathbf{X}^\top\boldsymbol{\alpha}).$$

Note that these are equivalent to (6.8) and (6.9) (once again assuming that $n\geqslant p$ and $\mathbf{X}$ has full rank p). Equivalently, the solution is found by solving (6.23):

$$\begin{bmatrix}\mathbf{X}\mathbf{X}^\top\mathbf{X}\mathbf{X}^\top+n\gamma\,\mathbf{X}\mathbf{X}^\top & \mathbf{X}\mathbf{X}^\top\mathbf{1}\\ \mathbf{1}^\top\mathbf{X}\mathbf{X}^\top & n\end{bmatrix}\begin{bmatrix}\boldsymbol{\alpha}\\ \eta_0\end{bmatrix}=\begin{bmatrix}\mathbf{X}\mathbf{X}^\top\\ \mathbf{1}^\top\end{bmatrix}\boldsymbol{y}.$$

This is a system of $(n+1)$ linear equations, and is typically of much larger dimension than the $(p+1)$ linear equations given by (6.8) and (6.9). As such, one may question the practicality of reformulating the problem in this way. However, the benefit of this formulation is that the problem can be expressed entirely through the Gram matrix $\mathbf{K}$, without having to explicitly compute the feature vectors — in turn permitting the (implicit) use of infinite dimensional feature spaces. ■

■ **Example 6.13 (Estimating the Peaks Function)** Figure 6.4 shows the surface plot of the *peaks* function:

$$f(x_1,x_2)=3(1-x_1)^2\mathrm{e}^{-x_1^2-(x_2+1)^2}-10\left(\frac{x_1}{5}-x_1^3-x_2^5\right)\mathrm{e}^{-x_1^2-x_2^2}-\frac{1}{3}\mathrm{e}^{-(x_1+1)^2-x_2^2}. \tag{6.24}$$

The goal is to learn the function $y=f(\boldsymbol{x})$ based on a small set of training data (pairs of $(\boldsymbol{x},y)$ values). The red dots in the figure represent data $\tau=\{(\boldsymbol{x}_i,y_i)\}_{i=1}^{20}$, where $y_i=f(\boldsymbol{x}_i)$ and the $\{\boldsymbol{x}_i\}$ have been chosen in a *quasi-random* way, using *Hammersley points* (with bases 2 QUASI-RANDOM

and 3) on the square $[-3,3]^2$. Quasi-random point sets have better space-filling properties than either a regular grid of points or a set of pseudo-random points. We refer to [71] for details. Note that there is no observation noise in this particular problem.

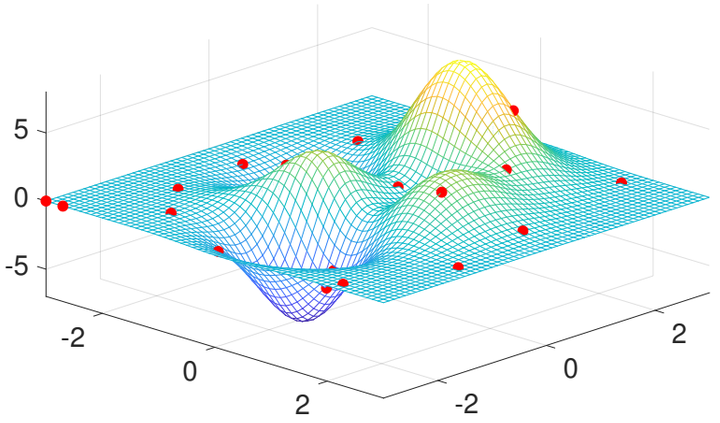


Figure 6.4: Peaks function sampled at 20 Hammersley points.

The purpose of this example is to illustrate how, using the small data set of size $n = 20$, the entire *peaks* function can be approximated well using kernel methods. In particular, we use the Gaussian kernel (6.15) on $\mathbb{R}^2$, and denote by $\mathcal{H}$ the unique RKHS corresponding to this kernel. We omit the regularization term in (6.19), and thus our objective is to find the solution to

$$\min_{g\in\mathcal{H}} \frac{1}{n}\sum_{i=1}^{n}(y_i - g(\boldsymbol{x}_i))^2.$$

By the representer theorem, the optimal function is of the form

$$g(\boldsymbol{x}) = \sum_{i=1}^{n} \alpha_i \exp\left(-\frac{1}{2}\frac{\|\boldsymbol{x}-\boldsymbol{x}_i\|^2}{\sigma^2}\right),$$

where $\boldsymbol{\alpha} := [\alpha_1,\ldots,\alpha_n]^\top$ is, by (6.23), the solution to the set of linear equations $\mathbf{K}\mathbf{K}^\top\boldsymbol{\alpha} = \mathbf{K}\boldsymbol{y}$.

Note that we are performing regression over the class of functions $\mathcal{H}$ with an implicit feature space. Due to the representer theorem, the solution to this problem coincides with the solution to the linear regression problem for which the i-th feature (for $i = 1,\ldots,n$) is chosen to be the vector $[\kappa(\boldsymbol{x}_1,\boldsymbol{x}_i),\ldots,\kappa(\boldsymbol{x}_n,\boldsymbol{x}_i)]^\top$.

The following code performs these calculations and gives the contour plots of g and the `peaks` functions, shown in Figure 6.5. We see that the two are quite close. Code for the generation of Hammersley points is available from the book's GitHub site as `genham.py`.

`peakskernel.py`

```
from genham import hammersley
import numpy as np
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D
```

```
from matplotlib import cm
from numpy.linalg import norm

import numpy as np
def peaks(x,y):
    z =  (3*(1-x)**2 * np.exp(-(x**2) - (y+1)**2)
          - 10*(x/5 - x**3 - y**5) * np.exp(-x**2 - y**2)
          - 1/3 * np.exp(-(x+1)**2 - y**2))
    return(z)

n = 20
x = -3 + 6*hammersley([2,3],n)
z = peaks(x[:,0],x[:,1])
xx, yy = np.mgrid[-3:3:150j,-3:3:150j]
zz = peaks(xx,yy)
plt.contour(xx,yy,zz,levels=50)

fig=plt.figure()
ax = fig.add_subplot(111,projection='3d')
ax.plot_surface(xx,yy,zz,rstride=1,cstride=1,color='c',alpha=0.3,
    linewidth=0)
ax.scatter(x[:,0],x[:,1],z,color='k',s=20)
plt.show()

sig2 = 0.3 # kernel parameter
def k(x,u):
    return(np.exp(-0.5*norm(x- u)**2/sig2))
K = np.zeros((n,n))
for i in range(n):
    for j in range(n):
        K[i,j] = k(x[i,:],x[j])
alpha = np.linalg.solve(K@K.T, K@z)



N, = xx.flatten().shape
Kx = np.zeros((n,N))
for i in range(n):
    for j in range(N):
        Kx[i,j] = k(x[i,:],np.array([xx.flatten()[j],yy.flatten()[j
            ]]))

g = Kx.T @ alpha
dim = np.sqrt(N).astype(int)
yhat = g.reshape(dim,dim)
plt.contour(xx,yy,yhat,levels=50)
```

6.6 Smoothing Cubic Splines

A striking application of kernel methods is to fitting "well-behaved" functions to data. Key examples of "well-behaved" functions are those that do not have large second-

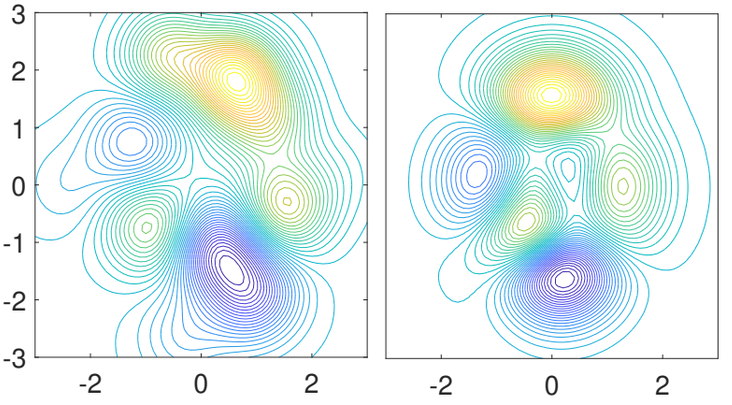


Figure 6.5: Contour plots for the prediction function g (left) and the *peaks* function given in (6.24) (right).

order derivatives. Consider functions $g : [0, 1] \to \mathbb{R}$ that are twice differentiable and define $\|g''\|^2 := \int_0^1 (g''(x))^2 \, \mathrm{d}x$ as a measure of the size of the second derivative.

■ **Example 6.14 (Behavior of $\|g''\|^2$)** Intuitively, the larger $\|g''\|^2$ is, the more "wiggly" the function g will be. As an explicit example, consider $g(x) = \sin(\omega x)$ for $x \in [0, 1]$, where ω is a free parameter. We can explicitly compute $g''(x) = -\omega^2 \sin(\omega x)$, and consequently

$$\|g''\|^2 = \int_0^1 \omega^4 \sin^2(\omega x) \, \mathrm{d}x = \frac{\omega^4}{2} \left(1 - \operatorname{sinc}(2\omega)\right).$$

As $|\omega| \to \infty$, the frequency of g increases and we have $\|g''\|^2 \to \infty$. ■

Now, in the context of data fitting, consider the following penalized least-squares optimization problem on $[0, 1]$:

$$\min_{g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^{n} (y_i - g(x_i))^2 + \gamma \|g''\|^2, \tag{6.25}$$

where we will specify $\mathcal{G}$ in what follows. In order to apply the kernel machinery, we want to write this in the form (6.19), for some RKHS $\mathcal{H}$ and null space $\mathcal{H}_0$. Clearly, the norm on $\mathcal{H}$ should be of the form $\|g\|_{\mathcal{H}} = \|g''\|$ and should be well-defined (i.e., finite and ensuring g and g' are absolutely continuous). This suggests that we take

$$\mathcal{H} = \{g \in L^2[0, 1] : \|g''\| < \infty, g, g' \text{ absolutely continuous}, \; g(0) = g'(0) = 0\},$$

with inner product

$$\langle f, g \rangle_{\mathcal{H}} := \int_0^1 f''(x) \, g''(x) \, \mathrm{d}x.$$

One rationale for imposing the boundary conditions $g(0) = g'(0) = 0$ is as follows: when expanding g about the point $x = 0$, Taylor's theorem (with integral remainder term) states that

$$g(x) = g(0) + g'(0) \, x + \int_0^x g''(s) \, (x - s) \, \mathrm{d}s.$$

Imposing the condition that $g(0) = g'(0) = 0$ for functions in $\mathcal{H}$ will ensure that $\mathcal{G} = \mathcal{H} \oplus \mathcal{H}_0$ where the null space $\mathcal{H}_0$ contains only linear functions, as we will see.

To see that this $\mathcal{H}$ is in fact an RKHS, we derive its reproducing kernel. Using integration by parts (or directly from the Taylor expansion above), write

$$g(x) = \int_0^x g'(s)\,\mathrm{d}s = \int_0^x g''(s)\,(x-s)\,\mathrm{d}s = \int_0^1 g''(s)\,(x-s)_+\,\mathrm{d}s.$$

If κ is a kernel, then by the reproducing property it must hold that

$$g(x) = \langle g, \kappa_x \rangle_{\mathcal{H}} = \int_0^1 g''(s)\,\kappa_x''(s)\,\mathrm{d}s,$$

so that κ must satisfy $\frac{\partial^2}{\partial s^2}\kappa(x,s) = (x-s)_+$, where $y_+ := \max\{y, 0\}$. Therefore, noting that $\kappa(x,u) = \langle \kappa_x, \kappa_u \rangle_{\mathcal{H}}$, we have (see Exercise 15)

$$\kappa(x,u) = \int_0^1 \frac{\partial^2 \kappa(x,s)}{\partial s^2}\frac{\partial^2 \kappa(u,s)}{\partial s^2}\,\mathrm{d}s = \frac{\max\{x,u\}\min\{x,u\}^2}{2} - \frac{\min\{x,u\}^3}{6}.$$

The last expression is a cubic function with quadratic and cubic terms that misses the constant and linear monomials. This is not surprising considering the Taylor's theorem interpretation of a function $g \in \mathcal{H}$. If we now take $\mathcal{H}_0$ as the space of functions of the following form (having zero second derivative):

$$h_0 = \eta_1 + \eta_2\, x, \quad x \in [0,1],$$

then (6.25) is exactly of the form (6.19).

As a consequence of the representer Theorem 6.6, the optimal solution to (6.25) is a linear combination of piecewise cubic functions:

$$g(x) = \eta_1 + \eta_2\, x + \sum_{i=1}^{n} \alpha_i\, \kappa(x_i, x). \tag{6.26}$$

Such a function is called a *cubic spline* with *n knots* (with one knot at each data point x_i) — so called, because the piecewise cubic function between knots is required to be "tied together" at the knots. The parameters $\boldsymbol{\alpha}, \boldsymbol{\eta}$ are determined from (6.21) for instance by solving (6.23) with matrices $\mathbf{K} = [\kappa(x_i, x_j)]_{i,j=1}^n$ and $\mathbf{Q}$ with i-th row of the form $[1, x_i]$ for $i = 1, \ldots, n$.

CUBIC SPLINE

■ **Example 6.15 (Smoothing Spline)** Figure 6.6 shows various cubic smoothing splines for the data $(0.05, 0.4), (0.2, 0.2), (0.5, 0.6), (0.75, 0.7), (1, 1)$. In the figure, we use the re-parameterization $r = 1/(1 + n\,\gamma)$ for the smoothing parameter. Thus $r \in [0, 1]$, where $r = 0$ means an infinite penalty for curvature (leading to the ordinary linear regression solution) and $r = 1$ does not penalize curvature at all and leads to a perfect fit via the so-called *natural spline*. Of course the latter will generally lead to overfitting. For r from 0 up to 0.8 the solutions will be close to the simple linear regression line, while only for r very close to 1, the shape of the curve changes significantly.

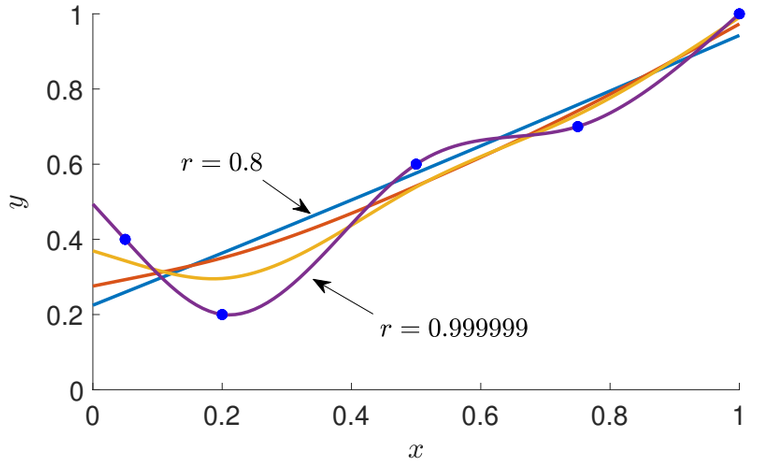


Figure 6.6: Various cubic smoothing splines for smoothing parameter $r = 1/(1 + n\gamma) \in \{0.8, 0.99, 0.999, 0.999999\}$. For $r = 1$, the natural spline through the data points is obtained; for $r = 0$, the simple linear regression line is found.

The following code first computes the matrices $\mathbf{K}$ and $\mathbf{Q}$, and then solves the linear system (6.23). Finally, the smoothing curve is determined via (6.26), for selected points, and then plotted. Note that the code plots only a single curve corresponding to the specified value of p.

smoothspline.py

```
import matplotlib.pyplot as plt
import numpy as np

x = np.array([[0.05, 0.2, 0.5, 0.75, 1.]]).T
y = np.array([[0.4, 0.2, 0.6, 0.7, 1.]]).T

n = x.shape[0]
r = 0.999
ngamma = (1-r)/r

k = lambda x1, x2 : (1/2)* np.max((x1,x2)) * np.min((x1,x2)) ** 2 \
                          - ((1/6)* np.min((x1,x2))**3)
K = np.zeros((n,n))
for i in range(n):
    for j in range(n):
        K[i,j] = k(x[i], x[j])

Q = np.hstack((np.ones((n,1)), x))

m1 = np.hstack((K @ K.T + (ngamma * K), K @ Q))
m2 = np.hstack((Q.T @ K.T, Q.T @ Q))
M = np.vstack((m1,m2))

c = np.vstack((K, Q.T)) @ y

ad = np.linalg.solve(M,c)
```

```
# plot the curve
xx = np.arange(0,1+0.01,0.01).reshape(-1,1)

g = np.zeros_like(xx)
Qx = np.hstack((np.ones_like(xx), xx))
g = np.zeros_like(xx)
N = np.shape(xx)[0]

Kx = np.zeros((n,N))
for i in range(n):
    for j in range(N):
        Kx[i,j] = k(x[i], xx[j])

g = g + np.hstack((Kx.T, Qx)) @ ad

plt.ylim((0,1.15))
plt.plot(xx, g, label = 'r = {}'.format(r), linewidth = 2)
plt.plot(x,y, 'b.', markersize=15)
plt.xlabel('$x$')
plt.ylabel('$y$')
plt.legend()
```

6.7 Gaussian Process Regression

Another application of the kernel machinery is to Gaussian process regression. A *Gaussian process* (GP) on a space $\mathcal{X}$ is a stochastic process $\{Z_{\boldsymbol{x}}, \boldsymbol{x} \in \mathcal{X}\}$ where, for any choice of indices $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, the vector $[Z_{\boldsymbol{x}_1}, \ldots Z_{\boldsymbol{x}_n}]^\top$ has a multivariate Gaussian distribution. As such, the distribution of a GP is completely specified by its mean and covariance functions $\mu : \mathcal{X} \to \mathbb{R}$ and $\kappa : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$, respectively. The covariance function is a finite positive semidefinite function, and hence, in view of Theorem 6.2, can be viewed as a reproducing kernel on $\mathcal{X}$.

GAUSSIAN PROCESS

As for ordinary regression, the objective of GP regression is to learn a regression function g that predicts a response $y = g(\boldsymbol{x})$ for each feature vector $\boldsymbol{x}$. This is done in a Bayesian fashion, by establishing (1) a prior pdf for g and (2) the likelihood of the data, for a given g. From these two we then derive, via Bayes' formula, the posterior distribution of g given the data. We refer to Section 2.9 for the general Bayesian framework.

☞ 168

☞ 47

A simple Bayesian model for GP regression is as follows. First, the prior distribution of g is taken to be the distribution of a GP with some known mean function μ and covariance function (that is, kernel) κ. Most often μ is taken to be a constant, and for simplicity of exposition, we take it to be 0. The Gaussian kernel (6.15) is often used for the covariance function. For radial basis function kernels (including the Gaussian kernel), points that are closer will be more highly correlated or "similar" [97], independent of translations in space.

Second, similar to standard regression, we view the observed feature vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ as fixed and the responses $y_1, \ldots, y_n$ as outcomes of random variables $Y_1, \ldots, Y_n$. Specifically, given g, we model the $\{Y_i\}$ as

$$Y_i = g(\boldsymbol{x}_i) + \varepsilon_i, \quad i = 1, \ldots, n, \tag{6.27}$$

where $\{\varepsilon_i\} \overset{\text{iid}}{\sim} \mathcal{N}(0, \sigma^2)$. To simplify the analysis, let us assume that σ^2 is known, so no prior needs to be specified for σ^2. Let $\boldsymbol{g} = [g(\boldsymbol{x}_1), \ldots, g(\boldsymbol{x}_n)]^\top$ be the (unknown) vector of regression values. Placing a GP prior on the function g is equivalent to placing a multivariate Gaussian prior on the vector $\boldsymbol{g}$:

$$\boldsymbol{g} \sim \mathcal{N}(\mathbf{0}, \mathbf{K}), \tag{6.28}$$

where the covariance matrix $\mathbf{K}$ of $\boldsymbol{g}$ is a Gram matrix (implicitly associated with a feature map through the kernel κ), given by:

$$\mathbf{K} = \begin{bmatrix} \kappa(\boldsymbol{x}_1, \boldsymbol{x}_1) & \kappa(\boldsymbol{x}_1, \boldsymbol{x}_2) & \ldots & \kappa(\boldsymbol{x}_1, \boldsymbol{x}_n) \\ \kappa(\boldsymbol{x}_2, \boldsymbol{x}_1) & \kappa(\boldsymbol{x}_2, \boldsymbol{x}_2) & \ldots & \kappa(\boldsymbol{x}_2, \boldsymbol{x}_n) \\ \vdots & \vdots & \ddots & \vdots \\ \kappa(\boldsymbol{x}_n, \boldsymbol{x}_1) & \kappa(\boldsymbol{x}_n, \boldsymbol{x}_2) & \ldots & \kappa(\boldsymbol{x}_n, \boldsymbol{x}_n) \end{bmatrix}. \tag{6.29}$$

The likelihood of our data given $\boldsymbol{g}$, denoted $p(\boldsymbol{y} \,|\, \boldsymbol{g})$, is obtained directly from the model (6.27):

$$(\boldsymbol{Y} \,|\, \boldsymbol{g}) \sim \mathcal{N}(\boldsymbol{g}, \sigma^2 \mathbf{I}_n). \tag{6.30}$$

Solving this Bayesian problem involves deriving the posterior distribution of $(\boldsymbol{g} \,|\, \boldsymbol{Y})$. To do so, we first note that since $\boldsymbol{Y}$ has covariance matrix $\mathbf{K} + \sigma^2 \mathbf{I}_n$ (which can be seen from (6.27)), the joint distribution of $\boldsymbol{Y}$ and $\boldsymbol{g}$ is again normal, with mean $\mathbf{0}$ and covariance matrix:

$$\mathbf{K}_{y,g} = \begin{bmatrix} \mathbf{K} + \sigma^2 \mathbf{I}_n & \mathbf{K} \\ \mathbf{K} & \mathbf{K} \end{bmatrix}. \tag{6.31}$$

☞ 438

The posterior can then be found by conditioning on $\boldsymbol{Y} = \boldsymbol{y}$, via Theorem C.8, giving

$$(\boldsymbol{g} \,|\, \boldsymbol{y}) \sim \mathcal{N}\left(\mathbf{K}^\top (\mathbf{K} + \sigma^2 \mathbf{I}_n)^{-1} \boldsymbol{y},\ \mathbf{K} - \mathbf{K}^\top (\mathbf{K} + \sigma^2 \mathbf{I}_n)^{-1} \mathbf{K}\right).$$

This only gives information about g at the observed points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. It is more interesting to consider the posterior predictive distribution of $\widetilde{g} := g(\widetilde{\boldsymbol{x}})$ for a new input $\widetilde{\boldsymbol{x}}$. We can find the corresponding posterior predictive pdf $p(\widetilde{g} \,|\, \boldsymbol{y})$ by integrating out the joint posterior pdf $p(\widetilde{g}, \boldsymbol{g} \,|\, \boldsymbol{y})$, which is equivalent to taking the expectation of $p(\widetilde{g} \,|\, \boldsymbol{g})$ when $\boldsymbol{g}$ is distributed according to the posterior pdf $p(\boldsymbol{g} \,|\, \boldsymbol{y})$; that is,

$$p(\widetilde{g} \,|\, \boldsymbol{y}) = \int p(\widetilde{g} \,|\, \boldsymbol{g})\, p(\boldsymbol{g} \,|\, \boldsymbol{y})\, \mathrm{d}\boldsymbol{g}.$$

To do so more easily than direct evaluation via the above integral representation of $p(\widetilde{g} \,|\, \boldsymbol{y})$, we can begin with the joint distribution of $[\boldsymbol{y}^\top, \widetilde{g}]^\top$, which is multivariate normal with mean $\mathbf{0}$ and covariance matrix

$$\widetilde{\mathbf{K}} = \begin{bmatrix} \mathbf{K} + \sigma^2 \mathbf{I}_n & \boldsymbol{\kappa} \\ \boldsymbol{\kappa}^\top & \kappa(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{x}}) \end{bmatrix}, \tag{6.32}$$

where $\boldsymbol{\kappa} = [\kappa(\widetilde{\boldsymbol{x}}, \boldsymbol{x}_1), \ldots, \kappa(\widetilde{\boldsymbol{x}}, \boldsymbol{x}_n)]^\top$. It now follows, again by using Theorem C.8, that $(\widetilde{g} \,|\, \boldsymbol{y})$ has a normal distribution with mean and variance given respectively by

$$\mu(\widetilde{\boldsymbol{x}}) = \boldsymbol{\kappa}^\top (\mathbf{K} + \sigma^2 \mathbf{I}_n)^{-1} \boldsymbol{y} \tag{6.33}$$

and

$$\sigma^2(\widetilde{\boldsymbol{x}}) = \kappa(\widetilde{\boldsymbol{x}}, \widetilde{\boldsymbol{x}}) - \boldsymbol{\kappa}^\top (\mathbf{K} + \sigma^2 \mathbf{I}_n)^{-1} \boldsymbol{\kappa}. \tag{6.34}$$

PREDICTIVE

These are sometimes called the *predictive* mean and variance. It is important to note that we are predicting the *expected* response $\mathbb{E}\widetilde{Y} = g(\widetilde{\boldsymbol{x}})$ here, and not the actual response $\widetilde{Y}$.

■ **Example 6.16 (GP Regression)** Suppose the regression function is

$$g(x) = 2\sin(2\pi x), \quad x \in [0, 1].$$

We use GP regression to estimate g, using a Gaussian kernel of the form (6.15) with bandwidth parameter 0.2. The explanatory variables $x_1, \ldots, x_{30}$ were drawn uniformly on the interval $[0, 1]$, and the responses were obtained from (6.27), with noise level $\sigma = 0.5$. Figure 6.7 shows 10 samples from the prior distribution for g as well as the data points and the true sinusoidal regression function g.

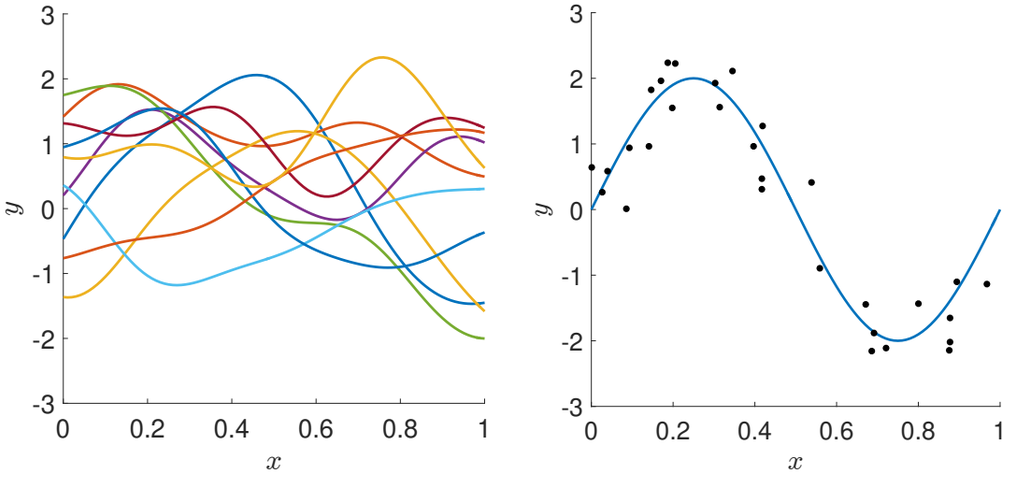


Figure 6.7: Left: samples drawn from the GP prior distribution. Right: the true regression function with the data points.

Again assuming that the variance σ^2, is known, the predictive distribution as determined by (6.33) and (6.34) is shown in Figure 6.8 for bandwidth 0.2 (left) and 0.02 (right). Clearly, decreasing the bandwidth leads to the covariance between points x and x' decreasing at a faster rate with respect to the squared distance $\|x - x'\|^2$, leading to a predictive mean that is less smooth. ■

In the above exposition, we have taken the mean function for the prior distribution of g to be identically zero. If instead we have a general mean function m and write $\boldsymbol{m} = [m(\boldsymbol{x}_1), \ldots, m(\boldsymbol{x}_n)]^\top$ then the predictive variance (6.34) remains unchanged, and the predictive mean (6.33) is modified to read

$$\mu(\widetilde{\boldsymbol{x}}) = m(\widetilde{\boldsymbol{x}}) + \boldsymbol{\kappa}^\top (\mathbf{K} + \sigma^2 \mathbf{I}_n)^{-1} (\boldsymbol{y} - \boldsymbol{m}) . \tag{6.35}$$

Typically, the variance σ^2 appearing in (6.27) is not known, and the kernel κ itself depends on several parameters — for instance a Gaussian kernel (6.15) with an unknown bandwidth parameter. In the Bayesian framework, one typically specifies a hierarchical model by introducing a prior $p(\boldsymbol{\theta})$ for the vector $\boldsymbol{\theta}$ of such *hyperparameters*. Now, the GP prior $(g \,|\, \boldsymbol{\theta})$ (equivalently, specifying $p(\boldsymbol{g} \,|\, \boldsymbol{\theta})$) and the model for the likelihood of the data given $\boldsymbol{Y}|\boldsymbol{g}, \boldsymbol{\theta}$, namely $p(\boldsymbol{y} \,|\, \boldsymbol{g}, \boldsymbol{\theta})$, are both dependent on $\boldsymbol{\theta}$. The posterior distribution of $(\boldsymbol{g} \,|\, \boldsymbol{y}, \boldsymbol{\theta})$ is as before.

HYPERPARAMETERS

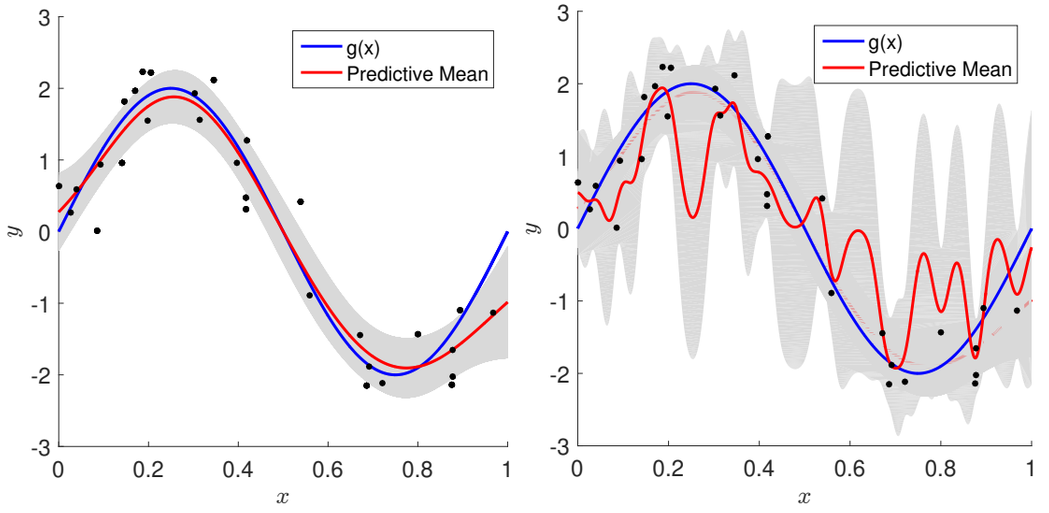


Figure 6.8: GP regression of synthetic data set with bandwidth 0.2 (left) and 0.02 (right). The black dots represent the data and the blue curve is the latent function $g(x) = 2\sin(2\pi x)$. The red curve is the mean of the GP predictive distribution given by (6.33), and the shaded region is the 95% confidence band, corresponding to the predictive variance given in (6.34).

One approach to setting the hyperparameter $\boldsymbol{\theta}$ is to determine its posterior $p(\boldsymbol{\theta} \,|\, \boldsymbol{y})$ and obtain a point estimate, for instance via its maximum a posteriori estimate. However, this can be a computationally demanding exercise. What is frequently done in practice is to consider instead the *marginal likelihood* $p(\boldsymbol{y} \,|\, \boldsymbol{\theta})$ and maximize this with respect to $\boldsymbol{\theta}$. This procedure is called *empirical Bayes*.

EMPIRICAL BAYES

Considering again the mean function m to be identically zero, from (6.31), we have that $(\boldsymbol{Y} \,|\, \boldsymbol{\theta})$ is multivariate normal with mean $\mathbf{0}$ and covariance matrix $\mathbf{K}_y = \mathbf{K} + \sigma^2 \mathbf{I}_n$, immediately giving an expression for the marginal log-likelihood:

$$\ln p(\boldsymbol{y} \,|\, \boldsymbol{\theta}) = -\frac{n}{2}\ln(2\pi) - \frac{1}{2}\ln|\det(\mathbf{K}_y)| - \frac{1}{2}\boldsymbol{y}^\top \mathbf{K}_y^{-1}\boldsymbol{y}. \tag{6.36}$$

We notice that only the second and third terms in (6.36) depend on $\boldsymbol{\theta}$. Considering a partial derivative of (6.36) with respect to a single element θ of the hyperparameter vector $\boldsymbol{\theta}$ yields

$$\frac{\partial}{\partial\theta}\ln p(\boldsymbol{y} \,|\, \boldsymbol{\theta}) = -\frac{1}{2}\mathrm{tr}\left(\mathbf{K}_y^{-1}\left[\frac{\partial}{\partial\theta}\mathbf{K}_y\right]\right) + \frac{1}{2}\boldsymbol{y}^\top \mathbf{K}_y^{-1}\left[\frac{\partial}{\partial\theta}\mathbf{K}_y\right]\mathbf{K}_y^{-1}\boldsymbol{y}, \tag{6.37}$$

where $\left[\frac{\partial}{\partial\theta}\mathbf{K}_y\right]$ is the element-wise derivative of matrix K_y with respect to θ. If these partial derivatives can be computed for each hyperparameter θ, gradient information could be used when maximizing (6.36).

■ **Example 6.17 (GP Regression (cont.))** Continuing Example 6.16, we plot in Figure 6.9 the marginal log-likelihood as a function of the noise level σ and bandwidth parameter.

The maximum is attained for a bandwidth parameter around 0.20 and $\sigma \approx 0.44$, which is very close to the left panel of Figure 6.8 for the case where σ was assumed to be known (and equal to 0.5). We note here that the marginal log-likelihood is extremely flat, perhaps owing to the small number of points. ■

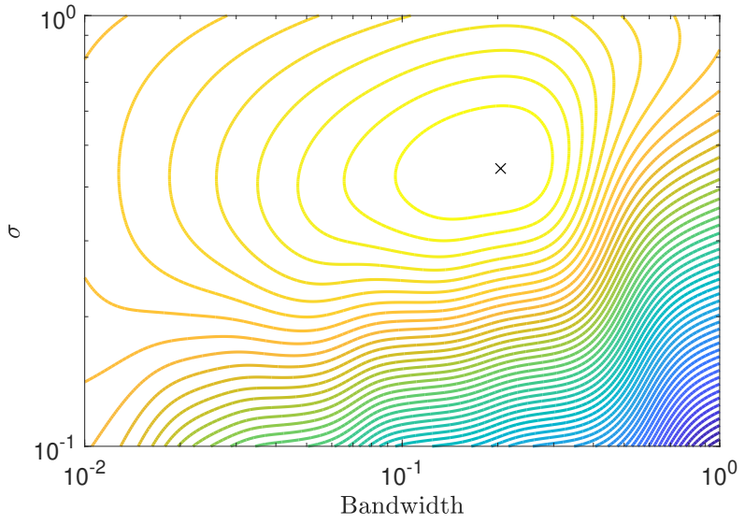


Figure 6.9: Contours of the marginal log-likelihood for the GP regression example. The maximum is denoted by a cross.

6.8 Kernel PCA

In its basic form, kernel PCA (principal component analysis) can be thought of as PCA in feature space. The main motivation for PCA introduced in Section 4.8 was as a dimensionality reduction technique. There, the analysis rested on an SVD of the matrix $\widehat{\boldsymbol{\Sigma}} = \frac{1}{n}\mathbf{X}^\top\mathbf{X}$, where the data in $\mathbf{X}$ was first centered via $x'_{i,j} = x_{i,j} - \overline{x}_j$ where $\overline{x}_i = \frac{1}{n}\sum_{i=1}^n x_{i,j}$. ☞ 153

What we shall do is to first re-cast the problem in terms of the Gram matrix $\mathbf{K} = \mathbf{X}\mathbf{X}^\top = [\langle \boldsymbol{x}_i, \boldsymbol{x}_j\rangle]$ (note the different order of $\mathbf{X}$ and $\mathbf{X}^\top$), and subsequently replace the inner product $\langle \boldsymbol{x}, \boldsymbol{x}'\rangle$ with $\kappa(\boldsymbol{x}, \boldsymbol{x}')$ for a general reproducing kernel κ. To make the link, let us start with an SVD of $\mathbf{X}^\top$:

$$\mathbf{X}^\top = \mathbf{U}\mathbf{D}\mathbf{V}^\top. \tag{6.38}$$

The dimensions of $\mathbf{X}^\top$, $\mathbf{U}$, $\mathbf{D}$, and $\mathbf{V}$ are $d \times n$, $d \times d$, $d \times n$, and $n \times n$, respectively. Then an SVD of $\mathbf{X}^\top\mathbf{X}$ is

$$\mathbf{X}^\top\mathbf{X} = (\mathbf{U}\mathbf{D}\mathbf{V}^\top)(\mathbf{U}\mathbf{D}\mathbf{V}^\top)^\top = \mathbf{U}(\mathbf{D}\mathbf{D}^\top)\mathbf{U}^\top$$

and an SVD of $\mathbf{K}$ is

$$\mathbf{K} = (\mathbf{U}\mathbf{D}\mathbf{V}^\top)^\top(\mathbf{U}\mathbf{D}\mathbf{V}^\top) = \mathbf{V}(\mathbf{D}^\top\mathbf{D})\mathbf{V}^\top.$$

Let $\lambda_1 \geqslant \cdots \geqslant \lambda_r > 0$ denote the non-zero eigenvalues of $\mathbf{X}^\top\mathbf{X}$ (or, equivalently, of $\mathbf{K}$) and denote the corresponding $r \times r$ diagonal matrix by $\boldsymbol{\Lambda}$. Without loss of generality we can assume that the eigenvector of $\mathbf{X}^\top\mathbf{X}$ corresponding to λ_k is the k-th column of $\mathbf{U}$ and that the k-th column of $\mathbf{V}$ is an eigenvector of $\mathbf{K}$. Similar to Section 4.8, let $\mathbf{U}_k$ and $\mathbf{V}_k$ contain the first k columns of $\mathbf{U}$ and $\mathbf{V}$, respectively, and let $\boldsymbol{\Lambda}_k$ be the corresponding $k \times k$ submatrix of $\boldsymbol{\Lambda}$, $k = 1, \ldots, r$. ☞ 153

By the SVD (6.38), we have $\mathbf{X}^\top\mathbf{V}_k = \mathbf{U}\mathbf{D}\mathbf{V}^\top\mathbf{V}_k = \mathbf{U}_k\boldsymbol{\Lambda}_k^{1/2}$. Next, consider the projection of a point $\boldsymbol{x}$ onto the k-dimensional linear space spanned by the columns of $\mathbf{U}_k$ — the first k principal components. We saw in Section 4.8 that this projection simply is the linear mapping $\boldsymbol{x} \mapsto \mathbf{U}_k^\top\boldsymbol{x}$. Using the fact that $\mathbf{U}_k = \mathbf{X}^\top\mathbf{V}_k\boldsymbol{\Lambda}^{-1/2}$, we find that $\boldsymbol{x}$ is projected to a

point z given by

$$z = \boldsymbol{\Lambda}_k^{-1/2} \mathbf{V}_k^\top \mathbf{X} \boldsymbol{x} = \boldsymbol{\Lambda}_k^{-1/2} \mathbf{V}_k^\top \boldsymbol{\kappa}_{\boldsymbol{x}},$$

where we have (suggestively) defined $\boldsymbol{\kappa}_{\boldsymbol{x}} := [\langle \boldsymbol{x}_1, \boldsymbol{x} \rangle, \ldots, \langle \boldsymbol{x}_n, \boldsymbol{x} \rangle]^\top$. The important point is that z is completely determined by the vector of inner products $\boldsymbol{\kappa}_{\boldsymbol{x}}$ and the k principal eigenvalues and (right) eigenvectors of the Gram matrix $\mathbf{K}$. Note that each component z_m of z is of the form

$$z_m = \sum_{i=1}^{n} \alpha_{m,i} \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}), \quad m = 1, \ldots, k. \tag{6.39}$$

The preceding discussion assumed centering of the columns of $\mathbf{X}$. Consider now an uncentered data matrix $\widetilde{\mathbf{X}}$. Then the centered data can be written as $\mathbf{X} = \widetilde{\mathbf{X}} - \frac{1}{n}\mathbf{E}_n \widetilde{\mathbf{X}}$, where $\mathbf{E}_n$ is the $n \times n$ matrix of ones. Consequently,

$$\mathbf{X}\mathbf{X}^\top = \widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top - \frac{1}{n}\mathbf{E}_n \widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top - \frac{1}{n}\widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top \mathbf{E}_n + \frac{1}{n^2}\mathbf{E}_n \widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top \mathbf{E}_n,$$

or, more compactly, $\mathbf{X}\mathbf{X}^\top = \mathbf{H}\widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top \mathbf{H}$, where $\mathbf{H} = \mathbf{I}_n - \frac{1}{n}\mathbf{1}_n \mathbf{1}_n^\top$, $\mathbf{I}_n$ is the $n \times n$ identity matrix, and $\mathbf{1}_n$ is the $n \times 1$ vector of ones.

To generalize to the kernel setting, we replace $\widetilde{\mathbf{X}}\widetilde{\mathbf{X}}^\top$ by $\mathbf{K} = [\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j), i, j = 1, \ldots, n]$ and set $\boldsymbol{\kappa}_{\boldsymbol{x}} = [\kappa(\boldsymbol{x}_1, \boldsymbol{x}), \ldots, \kappa(\boldsymbol{x}_n, \boldsymbol{x})]^\top$, so that $\boldsymbol{\Lambda}_k$ is the diagonal matrix of the k largest eigenvalues of $\mathbf{HKH}$ and $\mathbf{V}_k$ is the corresponding matrix of eigenvectors. Note that the "usual" PCA is recovered when we use the linear kernel $\kappa(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^\top \boldsymbol{y}$. However, instead of having only kernels that are explicitly inner products of feature vectors, we are now permitted to implicitly use *infinite* feature maps (functions) by using kernels.

■ **Example 6.18 (Kernel PCA)** We simulated 200 points, $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{200}$, from the uniform distribution on the set $B_1 \cup (B_4 \cap B_3^c)$, where $B_r := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leqslant r^2\}$ (disk with radius r). We apply kernel PCA with Gaussian kernel $\kappa(\boldsymbol{x}, \boldsymbol{x}') = \exp\left(-\|\boldsymbol{x} - \boldsymbol{x}'\|^2\right)$ and compute the functions $z_m(\boldsymbol{x}), m = 1, \ldots, 9$ in (6.39). Their density plots are shown in Figure 6.10. The data points are superimposed in each plot. From this we see that the principal components identify the radial structure present in the data. Finally, Figure 6.11 shows the projections $[z_1(\boldsymbol{x}_i), z_2(\boldsymbol{x}_i)]^\top, i = 1, \ldots, 200$ of the original data points onto the first two principal components. We see that the projected points can be separated by a straight line, whereas this is not possible for the original data; see also, Example 7.6 for a related problem.

☞ 274

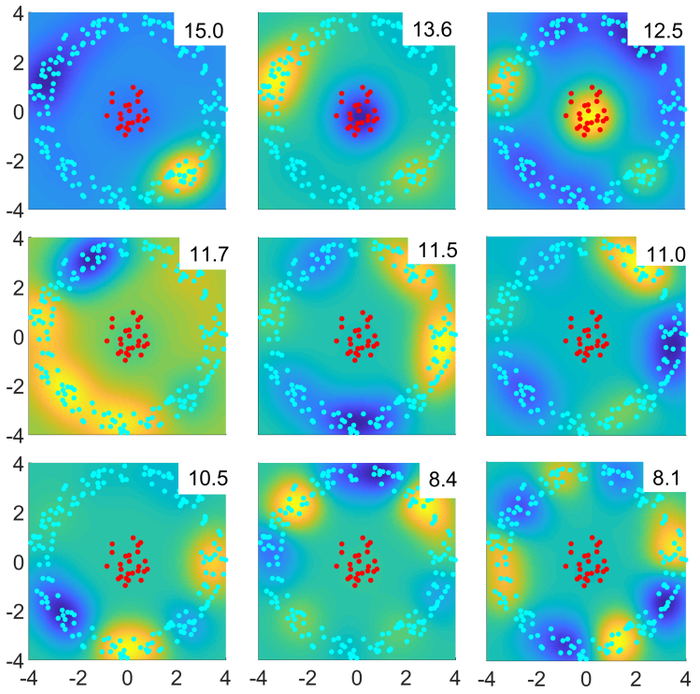


Figure 6.10: First nine eigenfunctions using a Gaussian kernel for the two-dimensional data set formed by the red and cyan points.

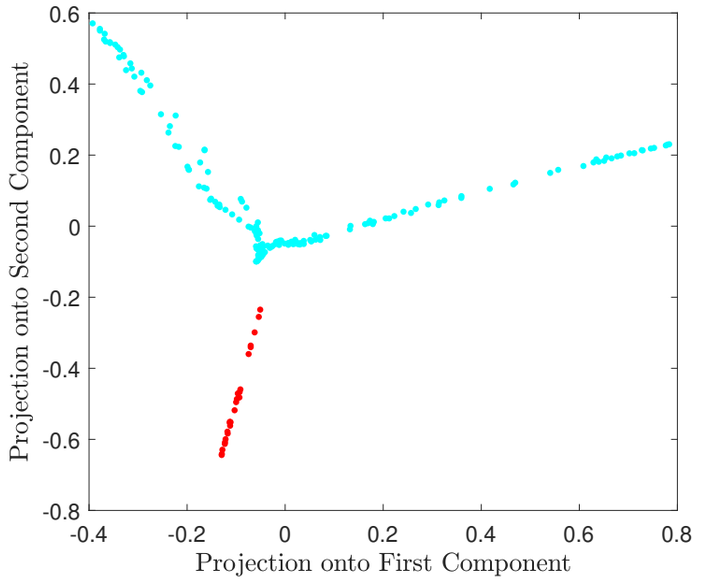


Figure 6.11: Projection of the data onto the first two principal components. Observe that already the projections of the inner and outer points are well separated.

Further Reading

For a good overview of the ridge regression and the lasso, we refer the reader to [36, 56]. For overviews of the theory of RKHS we refer to [3, 115, 126], and for in-depth background on splines and their connection to RKHSs we refer to [123]. For further details on GP regression we refer to [97] and for kernel PCA in particular we refer to [12, 92]. Finally, many facts about kernels and their corresponding RKHSs can be found in [115].

Exercises

1. Let $\mathcal{G}$ be an RKHS with reproducing kernel κ. Show that κ is a positive semidefinite function.

2. Show that a reproducing kernel, if it exists, is unique.

3. Let $\mathcal{G}$ be a Hilbert space of functions $g : \mathcal{X} \to \mathbb{R}$. Recall that the *evaluation functional* is the map $\delta_{\boldsymbol{x}} : g \mapsto g(\boldsymbol{x})$ for a given $\boldsymbol{x} \in \mathcal{X}$. Show that evaluation functionals are linear operators.

4. Let $\mathcal{G}_0$ be the pre-RKHS $\mathcal{G}_0$ constructed in the proof of Theorem 6.2. Thus, $g \in \mathcal{G}_0$ is of the form $g = \sum_{i=1}^{n} \alpha_i \kappa_{\boldsymbol{x}_i}$ and

$$\langle g, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}_0} = \sum_{i=1}^{n} \alpha_i \langle \kappa_{\boldsymbol{x}_i}, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}_0} = \sum_{i=1}^{n} \alpha_i \kappa(\boldsymbol{x}_i, \boldsymbol{x}) = g(\boldsymbol{x}).$$

   Therefore, we may write the evaluation functional of $g \in \mathcal{G}_0$ at $\boldsymbol{x}$ as $\delta_{\boldsymbol{x}} g := \langle g, \kappa_{\boldsymbol{x}} \rangle_{\mathcal{G}_0}$. Show that $\delta_{\boldsymbol{x}}$ is bounded on $\mathcal{G}_0$ for every $\boldsymbol{x}$; that is, $|\delta_{\boldsymbol{x}} f| < \gamma \, \|f\|_{\mathcal{G}_0}$, for some $\gamma < \infty$.

5. Continuing Exercise 4, let (f_n) be a Cauchy sequence in $\mathcal{G}_0$ such that $|f_n(\boldsymbol{x})| \to 0$ for all $\boldsymbol{x}$. Show that $\|f_n\|_{\mathcal{G}_0} \to 0$.

6. Continuing Exercises 5 and 4, to show that the inner product (6.14) is well defined, a number of facts have to be checked.

   (a) Verify that the limit converges.

   (b) Verify that the limit is independent of the Cauchy sequences used.

   (c) Verify that the properties of an inner product are satisfied. The only non-trivial property to verify is that $\langle f, f \rangle_{\mathcal{G}} = 0$ if and only if $f = 0$.

7. Exercises 4–6 show that $\mathcal{G}$ defined in the proof of Theorem 6.2 is an inner product space. It remains to prove that $\mathcal{G}$ is an RKHS. This requires us to prove that the inner product space $\mathcal{G}$ is complete (and thus Hilbert), and that its evaluation functionals are bounded and hence continuous (see Theorem A.16). This is done in a number of steps.

☞ 391

   (a) Show that $\mathcal{G}_0$ is dense in $\mathcal{G}$ in the sense that every $f \in \mathcal{G}$ is a limit point (with respect to the norm on $\mathcal{G}$) of a Cauchy sequence (f_n) in $\mathcal{G}_0$.

(b) Show that every evaluation functional $\delta_{\boldsymbol{x}}$ on $\mathcal{G}$ is continuous at the 0 function. That is,

$$\forall \varepsilon > 0 : \exists \delta > 0 : \forall f \in \mathcal{G} : \|f\|_{\mathcal{G}} < \delta \Rightarrow |f(\boldsymbol{x})| < \varepsilon. \tag{6.40}$$

Continuity of δ_x at all functions $g \in \mathcal{G}$ then follows automatically from linearity.

(c) Show that $\mathcal{G}$ is complete; that is, every Cauchy sequence $(f_n) \in \mathcal{G}$ converges in the norm $\|\cdot\|_{\mathcal{G}}$.

8. If κ_1 and κ_2 are kernels on $\mathcal{X}$ and $\mathcal{Y}$, then $\kappa_+((\boldsymbol{x},\boldsymbol{y}),(\boldsymbol{x}',\boldsymbol{y}')) := \kappa_1(\boldsymbol{x},\boldsymbol{x}') + \kappa_2(\boldsymbol{y},\boldsymbol{y}')$ and $\kappa_\times((\boldsymbol{x},\boldsymbol{y}),(\boldsymbol{x}',\boldsymbol{y}') := \kappa_1(\boldsymbol{x},\boldsymbol{x}')\kappa_2(\boldsymbol{y},\boldsymbol{y}')$ are kernels on the Cartesian product $\mathcal{X}\times\mathcal{Y}$. Prove this.

9. An RKHS enjoys the following desirable smoothness property: if (g_n) is a sequence belonging to RKHS $\mathcal{G}$ on $\mathcal{X}$, and $\|g_n - g\|_{\mathcal{G}} \to 0$, then $g(\boldsymbol{x}) = \lim_n g_n(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathcal{X}$. Prove this, using Cauchy–Schwarz.

10. Let $\boldsymbol{X}$ be an $\mathbb{R}^d$-valued random variable that is symmetric about the origin (that is, $\boldsymbol{X}$ and $(-\boldsymbol{X})$ are identically distributed). Denote by μ is its distribution and $\psi(\boldsymbol{t}) = \mathbb{E}\, \mathrm{e}^{\mathrm{i}\boldsymbol{t}^\top \boldsymbol{X}} = \int \mathrm{e}^{\mathrm{i}\boldsymbol{t}^\top \boldsymbol{x}}\, \mu(\mathrm{d}\boldsymbol{x})$ for $\boldsymbol{t} \in \mathbb{R}^d$ is its characteristic function. Verify that $\kappa(\boldsymbol{x},\boldsymbol{x}') = \psi(\boldsymbol{x}-\boldsymbol{x}')$ is a real-valued positive semidefinite function.

11. Suppose an RKHS $\mathcal{G}$ of functions from $\mathcal{X} \to \mathbb{R}$ (with kernel κ) is invariant under a group $\mathcal{T}$ of transformations $T : \mathcal{X} \to \mathcal{X}$; that is, for all $f, g \in \mathcal{G}$ and $T \in \mathcal{T}$, we have (i) $f \circ T \in \mathcal{G}$ and (ii) $\langle f \circ T, g \circ T\rangle_{\mathcal{G}} = \langle f, g\rangle_{\mathcal{G}}$. Show that $\kappa(T\boldsymbol{x}, T\boldsymbol{x}') = \kappa(\boldsymbol{x},\boldsymbol{x}')$ for all $\boldsymbol{x},\boldsymbol{x}' \in \mathcal{X}$ and $T \in \mathcal{T}$.

12. Given two Hilbert spaces $\mathcal{H}$ and $\mathcal{G}$, we call a mapping $A : \mathcal{H} \to \mathcal{G}$ a *Hilbert space isomorphism* if it is

HILBERT SPACE ISOMORPHISM

(i) a linear map; that is, $A(af + bg) = aA(f) + bA(g)$ for any $f, g \in \mathcal{H}$ and $a, b \in \mathbb{R}$.

(ii) a surjective map; and

(iii) an isometry; that is, for all $f, g \in \mathcal{H}$, it holds that $\langle f, g\rangle_{\mathcal{H}} = \langle Af, Ag\rangle_{\mathcal{G}}$.

Let $\mathcal{H} = \mathbb{R}^p$ (equipped with the usual Euclidean inner product) and construct its (continuous) *dual space* $\mathcal{G}$, consisting of all continuous linear functions from $\mathbb{R}^p$ to $\mathbb{R}$, as follows: (a) For each $\boldsymbol{\beta} \in \mathbb{R}^p$, define $g_{\boldsymbol{\beta}} : \mathbb{R}^p \to \mathbb{R}$ via $g_{\boldsymbol{\beta}}(\boldsymbol{x}) = \langle \boldsymbol{\beta}, \boldsymbol{x}\rangle = \boldsymbol{\beta}^\top \boldsymbol{x}$, for all $\boldsymbol{x} \in \mathbb{R}^p$. (b) Equip $\mathcal{G}$ with the inner product $\langle g_{\boldsymbol{\beta}}, g_{\boldsymbol{\gamma}}\rangle_{\mathcal{G}} := \boldsymbol{\beta}^\top \boldsymbol{\gamma}$.

Show that $A : \mathcal{H} \to \mathcal{G}$ defined by $A(\boldsymbol{\beta}) = g_{\boldsymbol{\beta}}$ for $\boldsymbol{\beta} \in \mathbb{R}^p$ is a Hilbert space isomorphism.

13. Let $\mathbf{X}$ be an $n \times p$ model matrix. Show that $\mathbf{X}^\top\mathbf{X} + n\gamma\mathbf{I}_p$ for $\gamma > 0$ is invertible.

14. As Example 6.8 clearly illustrates, the pdf of a random variable that is symmetric about the origin is not in general a valid reproducing kernel. Take two such iid random variables X and X' with common pdf f, and define $Z = X + X'$. Denote by ψ_Z and f_Z the characteristic function and pdf of Z, respectively.

Show that if ψ_Z is in $L^1(\mathbb{R})$, f_Z is a positive semidefinite function. Use this to show that $\kappa(x,x') = f_Z(x-x') = \mathbb{1}\{|x-x'| \leqslant 2\}(1 - |x-x'|/2)$ is a valid reproducing kernel.

15. For the smoothing cubic spline of Section 6.6, show that $\kappa(x,u) = \frac{\max\{x,u\}\min\{x,u\}^2}{2} - \frac{\min\{x,u\}^3}{6}$.

16. Let $\mathbf{X}$ be an $n \times p$ model matrix and let $\boldsymbol{u} \in \mathbb{R}^p$ be the unit-length vector with k-th entry equal to one ($u_k = \|\boldsymbol{u}\| = 1$). Suppose that the k-th column of $\mathbf{X}$ is $\boldsymbol{v}$ and that it is replaced with a new predictor $\boldsymbol{w}$, so that we obtain the new model matrix:

$$\widetilde{\mathbf{X}} = \mathbf{X} + (\boldsymbol{w} - \boldsymbol{v})\boldsymbol{u}^\top.$$

(a) Denoting

$$\boldsymbol{\delta} := \mathbf{X}^\top(\boldsymbol{w} - \boldsymbol{v}) + \frac{\|\boldsymbol{w} - \boldsymbol{v}\|^2}{2}\boldsymbol{u},$$

show that

$$\widetilde{\mathbf{X}}^\top\widetilde{\mathbf{X}} = \mathbf{X}^\top\mathbf{X} + \boldsymbol{u}\boldsymbol{\delta}^\top + \boldsymbol{\delta}\boldsymbol{u}^\top = \mathbf{X}^\top\mathbf{X} + \frac{(\boldsymbol{u}+\boldsymbol{\delta})(\boldsymbol{u}+\boldsymbol{\delta})^\top}{2} - \frac{(\boldsymbol{u}-\boldsymbol{\delta})(\boldsymbol{u}-\boldsymbol{\delta})^\top}{2}.$$

In other words, $\widetilde{\mathbf{X}}^\top\widetilde{\mathbf{X}}$ differs from $\mathbf{X}^\top\mathbf{X}$ by a symmetric matrix of rank two.

(b) Suppose that $\mathbf{B} := (\mathbf{X}^\top\mathbf{X} + n\gamma\mathbf{I}_p)^{-1}$ is already computed. Explain how the Sherman–Morrison formulas in Theorem A.10 can be applied twice to compute the inverse and log-determinant of the matrix $\widetilde{\mathbf{X}}^\top\widetilde{\mathbf{X}} + n\gamma\mathbf{I}_p$ in $O((n+p)p)$ computing time, rather than the usual $O((n+p^2)p)$ computing time.[3]

☞ 373

(c) Write a Python program for updating a matrix $\mathbf{B} = (\mathbf{X}^\top\mathbf{X} + n\gamma\mathbf{I}_p)^{-1}$ when we change the k-th column of $\mathbf{X}$, as shown in the following pseudo-code.

Algorithm 6.8.1: Updating via Sherman–Morrison Formula

input: Matrices $\mathbf{X}$ and $\mathbf{B}$, index k, and replacement $\boldsymbol{w}$ for the k-th column of $\mathbf{X}$.
output: Updated matrices $\mathbf{X}$ and $\mathbf{B}$.

Set $\boldsymbol{v} \in \mathbb{R}^n$ to be the k-th column of $\mathbf{X}$.
Set $\boldsymbol{u} \in \mathbb{R}^p$ to be the unit-length vector such that $u_k = \|\boldsymbol{u}\| = 1$.
$\mathbf{B} \leftarrow \mathbf{B} - \dfrac{\mathbf{B}\boldsymbol{u}\boldsymbol{\delta}^\top\mathbf{B}}{1 + \boldsymbol{\delta}^\top\mathbf{B}\boldsymbol{u}}$
$\mathbf{B} \leftarrow \mathbf{B} - \dfrac{\mathbf{B}\boldsymbol{\delta}\boldsymbol{u}^\top\mathbf{B}}{1 + \boldsymbol{u}^\top\mathbf{B}\boldsymbol{\delta}}$
Update the k-th column of $\mathbf{X}$ with $\boldsymbol{w}$.
return $\mathbf{X}, \mathbf{B}$

17. Use Algorithm 6.8.1 from Exercise 16 to write Python code that computes the ridge regression coefficient $\boldsymbol{\beta}$ in (6.5) and use it to replicate the results on Figure 6.1. The following pseudo-code (with running cost of $O((n+p)p^2)$) may help with the writing of the Python code.

☞ 217

[3] This Sherman–Morrison updating is not always numerically stable. A more numerically stable method will perform two consecutive rank-one updates of the Cholesky decomposition of $\mathbf{X}^\top\mathbf{X} + n\gamma\mathbf{I}_p$.

Algorithm 6.8.2: Ridge Regression Coefficients via Sherman–Morrison Formula

input: Training set $\{\mathbf{X}, \boldsymbol{y}\}$ and regularization parameter $\gamma > 0$.
output: Solution $\widehat{\boldsymbol{\beta}} = (n\gamma \mathbf{I}_p + \mathbf{X}^\top \mathbf{X})^{-1} \mathbf{X}^\top \boldsymbol{y}$.

```
Set A to be an n × p matrix of zeros and B ← (nγ I_p)^{-1}.
for j = 1, ..., p do
    Set w to be the j-th column of X.
    Update {A, B} via Algorithm 6.8.1 with inputs {A, B, j, w}.
β̂ ← B(X^⊤ y)
return β̂
```

18. Consider Example 2.10 with $\mathbf{D} = \operatorname{diag}(\lambda_1, \ldots, \lambda_p)$ for some nonnegative vector $\boldsymbol{\lambda} \in \mathbb{R}^p$, so that twice the negative logarithm of the *model evidence* can be written as ☞ 55

$$-2 \ln g(\boldsymbol{y}) = l(\boldsymbol{\lambda}) := n \ln[\boldsymbol{y}^\top (\mathbf{I} - \mathbf{X}\boldsymbol{\Sigma}\mathbf{X}^\top)\boldsymbol{y}] + \ln |\mathbf{D}| - \ln |\boldsymbol{\Sigma}| + c,$$

where c is a constant that depends only on n.

(a) Use the *Woodbury identities* (A.15) and (A.16) to show that ☞ 373

$$\begin{aligned} \mathbf{I} - \mathbf{X}\boldsymbol{\Sigma}\mathbf{X}^\top &= (\mathbf{I} + \mathbf{X}\mathbf{D}\mathbf{X}^\top)^{-1} \\ \ln |\mathbf{D}| - \ln |\Sigma| &= \ln |\mathbf{I} + \mathbf{X}\mathbf{D}\mathbf{X}^\top|. \end{aligned}$$

Deduce that $l(\boldsymbol{\lambda}) = n \ln[\boldsymbol{y}^\top \mathbf{C}\boldsymbol{y}] - \ln |\mathbf{C}| + c$, where $\mathbf{C} := (\mathbf{I} + \mathbf{X}\mathbf{D}\mathbf{X}^\top)^{-1}$.

(b) Let $[\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p] := \mathbf{X}$ denote the p columns/predictors of $\mathbf{X}$. Show that

$$\mathbf{C}^{-1} = \mathbf{I} + \sum_{k=1}^{p} \lambda_k \boldsymbol{v}_k \boldsymbol{v}_k^\top.$$

Explain why setting $\lambda_k = 0$ has the effect of excluding the k-th predictor from the regression model. How can this observation be used for model selection?

(c) Prove the following formulas for the gradient and Hessian elements of $l(\boldsymbol{\lambda})$:

$$\begin{aligned} \frac{\partial l}{\partial \lambda_i} &= \boldsymbol{v}_i^\top \mathbf{C} \boldsymbol{v}_i - n \frac{(\boldsymbol{v}_i^\top \mathbf{C}\boldsymbol{y})^2}{\boldsymbol{y}^\top \mathbf{C}\boldsymbol{y}} \\ \frac{\partial^2 l}{\partial \lambda_i \partial \lambda_j} &= (n-1)(\boldsymbol{v}_i^\top \mathbf{C}\boldsymbol{v}_j)^2 - n \left[\boldsymbol{v}_i^\top \mathbf{C}\boldsymbol{v}_j - \frac{(\boldsymbol{v}_i^\top \mathbf{C}\boldsymbol{y})(\boldsymbol{v}_j^\top \mathbf{C}\boldsymbol{y})}{\boldsymbol{y}^\top \mathbf{C}\boldsymbol{y}} \right]^2. \end{aligned} \tag{6.41}$$

(d) One method to determine which predictors in $\mathbf{X}$ are important is to compute

$$\boldsymbol{\lambda}^* := \operatorname*{argmin}_{\boldsymbol{\lambda} \geqslant \mathbf{0}} l(\boldsymbol{\lambda})$$

using, for example, the interior-point minimization Algorithm B.4.1 with gradient and Hessian computed from (6.41). Write Python code to compute $\boldsymbol{\lambda}^*$ and use it to select the best polynomial model in Example 2.10. ☞ 421

☞ 55

19. (Exercise 18 continued.) Consider again Example 2.10 with $\mathbf{D} = \operatorname{diag}(\lambda_1, \ldots, \lambda_p)$ for some nonnegative model-selection parameter $\boldsymbol{\lambda} \in \mathbb{R}^p$. A Bayesian choice for $\boldsymbol{\lambda}$ is the maximizer of the marginal likelihood $g(\boldsymbol{y} \mid \boldsymbol{\lambda})$; that is,

$$\boldsymbol{\lambda}^* = \operatorname*{argmax}_{\boldsymbol{\lambda} \geqslant \mathbf{0}} \iint g(\boldsymbol{\beta}, \sigma^2, \boldsymbol{y} \mid \boldsymbol{\lambda}) \, \mathrm{d}\boldsymbol{\beta} \, \mathrm{d}\sigma^2,$$

where

$$\ln g(\boldsymbol{\beta}, \sigma^2, \boldsymbol{y} \mid \boldsymbol{\lambda}) = -\frac{\|\boldsymbol{y} - \mathbf{X}\boldsymbol{\beta}\|^2 + \boldsymbol{\beta}^\top \mathbf{D}^{-1} \boldsymbol{\beta}}{2\sigma^2} - \frac{1}{2} \ln |\mathbf{D}| - \frac{n+p}{2} \ln(2\pi\sigma^2) - \ln \sigma^2.$$

☞ 128

To maximize $g(\boldsymbol{y} \mid \boldsymbol{\lambda})$, one can use the *EM algorithm* with $\boldsymbol{\beta}$ and σ^2 acting as *latent variables* in the *complete-data log-likelihood* $\ln g(\boldsymbol{\beta}, \sigma^2, \boldsymbol{y} \mid \boldsymbol{\lambda})$. Define

$$\begin{aligned} \boldsymbol{\Sigma} &:= (\mathbf{D}^{-1} + \mathbf{X}^\top \mathbf{X})^{-1} \\ \overline{\boldsymbol{\beta}} &:= \boldsymbol{\Sigma} \mathbf{X}^\top \boldsymbol{y} \\ \widehat{\sigma^2} &:= \left(\|\boldsymbol{y}\|^2 - \boldsymbol{y}^\top \mathbf{X} \overline{\boldsymbol{\beta}} \right) / n. \end{aligned} \tag{6.42}$$

(a) Show that the conditional density of the latent variables $\boldsymbol{\beta}$ and σ^2 is such that

$$\begin{aligned} \left(\sigma^{-2} \,\middle|\, \boldsymbol{\lambda}, \boldsymbol{y} \right) &\sim \mathsf{Gamma}\left(\frac{n}{2}, \frac{n}{2} \widehat{\sigma^2} \right) \\ \left(\boldsymbol{\beta} \,\middle|\, \boldsymbol{\lambda}, \sigma^2, \boldsymbol{y} \right) &\sim \mathcal{N}\left(\overline{\boldsymbol{\beta}}, \, \sigma^2 \boldsymbol{\Sigma} \right). \end{aligned}$$

☞ 432

(b) Use Theorem C.2 to show that the expected complete-data log-likelihood is

$$-\frac{\overline{\boldsymbol{\beta}}^\top \mathbf{D}^{-1} \overline{\boldsymbol{\beta}}}{2\widehat{\sigma^2}} - \frac{\operatorname{tr}(\mathbf{D}^{-1}\boldsymbol{\Sigma}) + \ln |\mathbf{D}|}{2} + c_1,$$

where c_1 is a constant that does not depend on $\boldsymbol{\lambda}$.

☞ 361

(c) Use Theorem A.2 to simplify the expected complete-data log-likelihood and to show that it is maximized at $\lambda_i = \boldsymbol{\Sigma}_{ii} + (\overline{\beta}_i / \widehat{\sigma})^2$ for $i = 1, \ldots, p$. Hence, deduce the following E and M steps in the EM algorithm:

E-step. Given $\boldsymbol{\lambda}$, update $(\boldsymbol{\Sigma}, \overline{\boldsymbol{\beta}}, \widehat{\sigma^2})$ via the formulas (6.42).

M-step. Given $(\boldsymbol{\Sigma}, \overline{\boldsymbol{\beta}}, \widehat{\sigma^2})$, update $\boldsymbol{\lambda}$ via $\lambda_i = \boldsymbol{\Sigma}_{ii} + (\overline{\beta}_i / \widehat{\sigma})^2, \;\; i = 1, \ldots, p$.

(d) Write Python code to compute $\boldsymbol{\lambda}^*$ via the EM algorithm, and use it to select the best polynomial model in Example 2.10. A possible stopping criterion is to terminate the EM iterations when

$$\ln g(\boldsymbol{y} \mid \boldsymbol{\lambda}_{t+1}) - \ln g(\boldsymbol{y} \mid \boldsymbol{\lambda}_t) < \varepsilon$$

for some small $\varepsilon > 0$, where the marginal log-likelihood is

$$\ln g(\boldsymbol{y} \mid \boldsymbol{\lambda}) = -\frac{n}{2} \ln(n\pi\widehat{\sigma^2}) - \frac{1}{2} \ln |\mathbf{D}| + \frac{1}{2} \ln |\boldsymbol{\Sigma}| + \ln \Gamma(n/2).$$

20. In this exercise we explore how the *early stopping* of the *gradient descent* iterations (see Example B.10), ☞ 414

$$\boldsymbol{x}_{t+1} = \boldsymbol{x}_t - \alpha \nabla f(\boldsymbol{x}_t), \quad t = 0, 1, \ldots,$$

is (approximately) equivalent to the global minimization of $f(\boldsymbol{x}) + \frac{1}{2}\gamma\|\boldsymbol{x}\|^2$ for certain values of the *ridge regularization* parameter $\gamma > 0$ (see Example 6.1). We illustrate the *early stopping* idea on the quadratic function $f(\boldsymbol{x}) = \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu})^\top \mathbf{H}(\boldsymbol{x} - \boldsymbol{\mu})$, where $\mathbf{H} \in \mathbb{R}^{n \times n}$ is a symmetric positive-definite (Hessian) matrix with eigenvalues $\{\lambda_k\}_{k=1}^n$. EARLY STOPPING

(a) Verify that for a symmetric matrix $\mathbf{A} \in \mathbb{R}^n$ such that $\mathbf{I} - \mathbf{A}$ is invertible, we have

$$\mathbf{I} + \mathbf{A} + \cdots + \mathbf{A}^{t-1} = (\mathbf{I} - \mathbf{A}^t)(\mathbf{I} - \mathbf{A})^{-1}.$$

(b) Let $\mathbf{H} = \mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^\top$ be the diagonalization of $\mathbf{H}$ as per Theorem A.8. If $\boldsymbol{x}_0 = \mathbf{0}$, show that the formula for $\boldsymbol{x}_t$ is ☞ 368

$$\boldsymbol{x}_t = \boldsymbol{\mu} - \mathbf{Q}(\mathbf{I} - \alpha\boldsymbol{\Lambda})^t \mathbf{Q}^\top \boldsymbol{\mu}.$$

Hence, deduce that a necessary condition for $\boldsymbol{x}_t$ to converge is $\alpha < 2/\max_k \lambda_k$.

(c) Show that the minimizer of $f(\boldsymbol{x}) + \frac{1}{2}\gamma\|\boldsymbol{x}\|^2$ can be written as

$$\boldsymbol{x}^* = \boldsymbol{\mu} - \mathbf{Q}(\mathbf{I} + \gamma^{-1}\boldsymbol{\Lambda})^{-1}\mathbf{Q}^\top \boldsymbol{\mu}.$$

(d) For a fixed value of t, let the learning rate $\alpha \downarrow 0$. Using part (b) and (c), show that if $\gamma \simeq 1/(t\,\alpha)$ as $\alpha \downarrow 0$, then $\boldsymbol{x}_t \simeq \boldsymbol{x}^*$. In other words, $\boldsymbol{x}_t$ is approximately equal to $\boldsymbol{x}^*$ for small α, provided that γ is inversely proportional to $t\,\alpha$.

CHAPTER 7

CLASSIFICATION

The purpose of this chapter is to explain the mathematical ideas behind well-known classification techniques such as the naïve Bayes method, linear and quadratic discriminant analysis, logistic/softmax classification, the K-nearest neighbors method, and support vector machines.

7.1 Introduction

Classification methods are supervised learning methods in which a categorical *response* variable Y takes one of c possible values (for example whether a person is sick or healthy), which is to be predicted from a vector $\boldsymbol{X}$ of *explanatory* variables (for example, the blood pressure, age, and smoking status of the person), using a *prediction function* g. In this sense, g classifies the input $\boldsymbol{X}$ into one of the classes, say in the set $\{0, \ldots, c-1\}$. For this reason, we will call g a *classification function* or simply *classifier*. As with any supervised learning technique (see Section 2.3), the goal is to minimize the expected loss or *risk*

CLASSIFIER

$$\ell(g) = \mathbb{E}\,\mathrm{Loss}(Y, g(\boldsymbol{X})) \tag{7.1}$$

for some loss function, $\mathrm{Loss}(y, \widehat{y})$, that quantifies the impact of classifying a response y via $\widehat{y} = g(\boldsymbol{x})$. The natural loss function is the *zero–one* (also written 0–1) or *indicator loss*: $\mathrm{Loss}(y, \widehat{y}) := \mathbb{1}\{y \neq \widehat{y}\}$; that is, there is no loss for a correct classification ($y = \widehat{y}$) and a unit loss for a misclassification ($y \neq \widehat{y}$). In this case the optimal classifier g^* is given in the following theorem.

INDICATOR LOSS

Theorem 7.1: Optimal classifier

For the loss function $\mathrm{Loss}(y, \widehat{y}) = \mathbb{1}\{y \neq \widehat{y}\}$, an optimal classification function is

$$g^*(\boldsymbol{x}) = \operatorname*{argmax}_{y \in \{0,\ldots,c-1\}} \mathbb{P}[Y = y \,|\, \boldsymbol{X} = \boldsymbol{x}]. \tag{7.2}$$

Proof: The goal is to minimize $\ell(g) = \mathbb{E}\,\mathbb{1}\{Y \neq g(\boldsymbol{X})\}$ over all functions g taking values in $\{0, \ldots, c-1\}$. Conditioning on $\boldsymbol{X}$ gives, by the tower property, $\ell(g) = \mathbb{E}\,(\mathbb{P}[Y \neq g(\boldsymbol{X}) \,|\, \boldsymbol{X}]\,)$, and so minimizing $\ell(g)$ with respect to g can be accomplished by *maximizing* $\mathbb{P}[Y =$ ☞ 433

$g(\boldsymbol{x}) \,|\, \boldsymbol{X} = \boldsymbol{x}]$ with respect to $g(\boldsymbol{x})$, for every fixed $\boldsymbol{x}$. In other words, take $g(\boldsymbol{x})$ to be equal to the class label y for which $\mathbb{P}[Y = y \,|\, \boldsymbol{X} = \boldsymbol{x}]$ is maximal. □

The formulation (7.2) allows for "ties", when there is an equal probability between optimal classes for a feature vector $\boldsymbol{x}$. Assigning one of these tied classes arbitrarily (or randomly) to $\boldsymbol{x}$ does not affect the loss function and so we assume for simplicity that $g^*(\boldsymbol{x})$ is always a scalar value.

☞ 21

Note that, as was the case for the regression (see, e.g., Theorem 2.1), the optimal prediction function depends on the conditional pdf $f(y \,|\, \boldsymbol{x}) = \mathbb{P}[Y = y \,|\, \boldsymbol{X} = \boldsymbol{x}]$. However, since we assign $\boldsymbol{x}$ to class y if $f(y \,|\, \boldsymbol{x}) \geqslant f(z \,|\, \boldsymbol{x})$ for all z, we do not need to learn the entire surface of the function $f(y \,|\, \boldsymbol{x})$; we only need to estimate it well enough near the decision boundary $\{\boldsymbol{x} : f(y \,|\, \boldsymbol{x}) = f(z \,|\, \boldsymbol{x})\}$ for any choice of classes y and z. This is because the assignment (7.2) divides the feature space into c regions, $\mathcal{R}_y = \{\boldsymbol{x} : f(y \,|\, \boldsymbol{x}) = \max_z f(z \,|\, \boldsymbol{x})\}$, $y = 0, \ldots, c-1$.

Recall that for any supervised learning problem the smallest possible expected loss (that is, the irreducible risk) is given by $\ell^* = \ell(g^*)$. For the indicator loss, the irreducible risk is equal to $\mathbb{P}[Y \neq g^*(\boldsymbol{X})]$. This smallest possible probability of misclassification is often called the *Bayes error rate*.

BAYES ERROR RATE

For a given training set τ, a classifier is often derived from a *pre-classifier* g_τ, which is a prediction function (learner) that can take any real value, rather than only values in the set of class labels. A typical situation is the case of binary classification with labels -1 and 1, where the prediction function g_τ is a function taking values in the interval $[-1, 1]$ and the actual classifier is given by $\operatorname{sign}(g_\tau)$. It will be clear from the context whether a prediction function g_τ should be interpreted as a classifier or pre-classifier.

The indicator loss function may not always be the most appropriate choice of loss function for a given classification problem. For example, when diagnosing an illness, the mistake in misclassifying a person as being sick when in fact the person is healthy may be less serious than classifying the person as healthy when in fact the person is sick. In Section 7.2 we consider various classification metrics.

There are many ways to fit a classifier to a training set $\tau = \{(\boldsymbol{x}_1, y_1), \ldots, (\boldsymbol{x}_n, y_n)\}$. The approach taken in Section 7.3 is to use a Bayesian framework for classification. Here the conditional pdf $f(y \,|\, \boldsymbol{x})$ is viewed as a posterior pdf $f(y \,|\, \boldsymbol{x}) \propto f(\boldsymbol{x} \,|\, y) f(y)$ for a given class prior $f(y)$ and likelihood $f(\boldsymbol{x} \,|\, y)$. Section 7.4 discusses linear and quadratic discriminant analysis for classification, which assumes that the class of approximating functions for the conditional pdf $f(\boldsymbol{x} \,|\, y)$ is a parametric class $\mathcal{G}$ of Gaussian densities. As a result of this choice of $\mathcal{G}$, the marginal $f(\boldsymbol{x})$ is approximated via a Gaussian mixture density.

In contrast, in the logistic or soft-max classification in Section 7.5, the conditional pdf $f(y \,|\, \boldsymbol{x})$ is approximated using a more flexible class of approximating functions. As a result of this, the approximation to the marginal density $f(\boldsymbol{x})$ does not belong to a simple parametric class (such as a Gaussian mixture). As in unsupervised learning, the cross-entropy loss is the most common choice for training the learner.

The K-nearest neighbors method, discussed in Section 7.6, is yet another approach to classification that makes minimal assumptions on the class $\mathcal{G}$. Here the aim is to directly

estimate the conditional pdf $f(y \mid \boldsymbol{x})$ from the training data, using only feature vectors in the neighborhood of $\boldsymbol{x}$. In Section 7.7 we explain the support vector methodology for classification; this is based on the same Reproducing Kernel Hilbert Space ideas that proved successful for regression analysis in Section 6.3. Finally, a versatile way to do both classification and regression is to use classification and regression trees. This is the topic of Chapter 8. Neural networks (Chapter 9) provide yet another way to perform classification.

☞ 222
☞ 289
☞ 325

7.2 Classification Metrics

The effectiveness of a classifier g is, theoretically, measured in terms of the risk (7.1), which depends on the loss function used. Fitting a classifier to iid training data $\tau = \{(\boldsymbol{x}_i, y_i)\}_{i=1}^n$ is established by minimizing the *training loss*

$$\ell_\tau(g) = \frac{1}{n} \sum_{i=1}^{n} \text{Loss}(y_i, g(\boldsymbol{x}_i)) \tag{7.3}$$

over some class of functions $\mathcal{G}$. As the training loss is often a poor estimator of the risk, the risk is usually estimated as in (7.3), using instead a test set $\tau' = \{(\boldsymbol{x}'_i, y'_i)\}_{i=1}^{n'}\}$ that is independent of the training set, as explained in Section 2.3. To measure the performance of a classifier on a training or test set, it is convenient to introduce the notion of a *loss matrix*. Consider a classification problem with classifier g, loss function Loss, and classes $0, \ldots, c-1$. If an input feature vector $\boldsymbol{x}$ is classified as $\widehat{y} = g(\boldsymbol{x})$ when the observed class is y, the loss incurred is, by definition, $\text{Loss}(y, \widehat{y})$. Consequently, we may identify the loss function with a matrix $\mathbf{L} = [\text{Loss}(j,k), j,k \in \{0,\ldots,c-1\}]$. For the indicator loss function, the matrix $\mathbf{L}$ has 0s on the diagonal and 1s everywhere else. Another useful matrix is the *confusion matrix*, denoted by $\mathbf{M}$, where the (j,k)-th element of $\mathbf{M}$ counts the number of times that, for the training or test data, the actual (observed) class is j whereas the predicted class is k. Table 7.1 shows the confusion matrix of some Dog/Cat/Possum classifier.

☞ 23

LOSS MATRIX

CONFUSION MATRIX

Table 7.1: Confusion matrix for three classes.

	Predicted		
Actual	Dog	Cat	Possum
Dog	30	2	6
Cat	8	22	15
Possum	7	4	41

We can now express the classifier performance (7.3) in terms of $\mathbf{L}$ and $\mathbf{M}$ as

$$\frac{1}{n} \sum_{j,k} [\mathbf{L} \odot \mathbf{M}]_{jk}, \tag{7.4}$$

where $\mathbf{L} \odot \mathbf{M}$ is the elementwise product of $\mathbf{L}$ and $\mathbf{M}$. Note that for the indicator loss, (7.4) is simply $1 - \text{tr}(\mathbf{M})/n$, and is called the *misclassification error*. The expression (7.4) makes it clear that both the counts and the loss are important in determining the performance of a classifier.

MISCLASSIFICATION ERROR

☞ 461

TRUE POSITIVE

TRUE NEGATIVE

FALSE POSITIVE

FALSE NEGATIVE

In the spirit of Table C.4 for hypothesis testing, it is sometimes useful to divide the elements of a confusion matrix into four groups. The diagonal elements are the *true positive* counts; that is, the numbers of correct classifications for each class. The true positive counts for the Dog, Cat, and Possum classes in Table 7.1 are 30, 22, and 41, respectively. Similarly, the *true negative* count for a class is the sum of all matrix elements that do not belong to the row or the column of this particular class. For the Dog class it is $22+15+4+41 = 82$. The *false positive* count for a class is the sum of the corresponding column elements without the diagonal element. For the Dog class it is $8 + 7 = 15$. Finally, the *false negative* count for a specific class, can be calculated by summing over the corresponding row elements (again, without counting the diagonal element). For the Dog class it is $2 + 6 = 8$.

In terms of the elements of the confusion matrix, we have the following counts for class $j = 0, \ldots, c-1$:

$$\begin{aligned}
&\text{True positive} && \mathrm{tp}_j = \mathbf{M}_{jj}, && \\
&\text{False positive} && \mathrm{fp}_j = \sum_{k \neq j} \mathbf{M}_{kj}, && \text{(column sum)} \\
&\text{False negative} && \mathrm{fn}_j = \sum_{k \neq j} \mathbf{M}_{jk}, && \text{(row sum)} \\
&\text{True negative} && \mathrm{tn}_j = n - \mathrm{fn}_j - \mathrm{fp}_j - \mathrm{tp}_j. &&
\end{aligned}$$

Note that in the binary classification case ($c = 2$), and using the indicator loss function, the misclassification error (7.4) can be written as

$$\mathrm{error}_j = \frac{\mathrm{fp}_j + \mathrm{fn}_j}{n}. \tag{7.5}$$

This does not depend on which of the two classes is considered, as $\mathrm{fp}_0 + \mathrm{fn}_0 = \mathrm{fp}_1 + \mathrm{fn}_1$.

ACCURACY

Similarly, the *accuracy* measures the fraction of correctly classified objects:

$$\mathrm{accuracy}_j = 1 - \mathrm{error}_j = \frac{\mathrm{tp}_j + \mathrm{tn}_j}{n}. \tag{7.6}$$

In some cases, classification error (or accuracy) alone is not sufficient to adequately describe the effectiveness of a classifier. As an example, consider the following two classification problems based on a fingerprint detection system:

1. Identification of authorized personnel in a top-secret military facility.
2. Identification to get an online discount for some retail chain.

Both problems are binary classification problems. However, a false positive in the first problem is extremely dangerous, while a false positive in the second problem will make a customer happy. Let us examine a classifier in the top-secret facility. The corresponding confusion matrix is given in Table 7.2.

Table 7.2: Confusion matrix for authorized personnel classification.

	Predicted	
Actual	authorized	non-authorized
authorized	100	400
non-authorized	50	100,000

From (7.6), we conclude that the accuracy of classification is equal to

$$\text{accuracy} = \frac{\text{tp} + \text{tn}}{\text{tp} + \text{tn} + \text{fp} + \text{fn}} = \frac{100 + 100,000}{100 + 100,000 + 50 + 400} \approx 99.55\%.$$

However, we can see that in this particular case, accuracy is a problematic metric, since the algorithm allowed 50 non-authorized personnel to enter the facility. One way to deal with this issue is to modify the loss function to give a much higher loss to non-authorized access. Thus, instead of an (indicator) loss matrix, we could for example take the loss matrix

$$\mathbf{L} = \begin{pmatrix} 0 & 1 \\ 1000 & 0 \end{pmatrix}.$$

An alternative approach is to keep the indicator loss function and consider additional classification metrics. Below we give a list of commonly used metrics. For simplicity we call an object whose actual class is j a "j-object".

- The *precision* (also called *positive predictive value*) is the fraction of all objects classified as j that are actually j-objects. Specifically, PRECISION

$$\text{precision}_j = \frac{\text{tp}_j}{\text{tp}_j + \text{fp}_j}.$$

- The *recall* (also called *sensitivity*) is the fraction of all j-objects that are correctly classified as such. That is, RECALL

$$\text{recall}_j = \frac{\text{tp}_j}{\text{tp}_j + \text{fn}_j}.$$

- The *specificity* measures the fraction of all non-j-objects that are correctly classified as such. Specifically, SPECIFICITY

$$\text{specificity}_j = \frac{\text{tn}_j}{\text{fp}_j + \text{tn}_j}.$$

- The F_β *score* is a combination of the precision and the recall and is used as a single measurement for a classifier's performance. The F_β score is given by F_β SCORE

$$F_{\beta,j} = \frac{(\beta^2 + 1)\,\text{tp}_j}{(\beta^2 + 1)\,\text{tp}_j + \beta^2\,\text{fn}_j + \text{fp}_j}.$$

  For $\beta = 0$ we obtain the precision and for $\beta \to \infty$ we obtain the recall.

The particular choice of metric is clearly application dependent. For example, in the classification of authorized personnel in a top-secret military facility, suppose we have two classifiers. The first (Classifier 1) has a confusion matrix given in Table 7.2, and the second (Classifier 2) has a confusion matrix given in Table 7.3. Various metrics for these two classifiers are show in Table 7.4. In this case we prefer Classifier 1, which has a much higher precision.

Table 7.3: Confusion matrix for authorized personnel classification, using a different classifier (Classifier 2).

	Predicted	
Actual	Authorized	Non-Authorized
authorized	50	10
non-authorized	450	100,040

Table 7.4: Comparing the metrics for the confusion matrices in Tables 7.2 and 7.3.

Metric	Classifier 1	Classifier 2
accuracy	9.955×10^{-1}	9.954×10^{-1}
precision	$\mathbf{6.667 \times 10^{-1}}$	$\mathbf{1.000 \times 10^{-1}}$
recall	2.000×10^{-1}	8.333×10^{-1}
specificity	9.995×10^{-1}	9.955×10^{-1}
F_1	3.077×10^{-1}	1.786×10^{-1}

■ **Remark 7.1 (Multilabel and Hierarchical Classification)** In standard classification the classes are assumed to be mutually exclusive. For example a satellite image could be classified as "cloudy", "clear", or "foggy". In *multilabel classification* the classes (often called labels) do not have to be mutually exclusive. In this case the response is a subset $\mathcal{Y}$ of some collection of labels $\{0, \ldots, c-1\}$. Equivalently, the response can be viewed as a binary vector of length c, where the y-th element is 1 if the response belongs to label y and 0 otherwise. Again, consider the satellite image example and add two labels, such as "road" and "river" to the previous three labels. Clearly, an image can contain both a road and a river. In addition, the image can be clear, cloudy, or foggy.

MULTILABEL CLASSIFICATION

In *hierarchical classification* a hierarchical relation between classes/labels is taken into account during the classification process. Usually, the relations are modeled via a tree or a directed acyclic graph. A visual comparison between the hierarchical and non-hierarchical (flat) classification tasks for satellite image data is presented in Figure 7.1.

HIERARCHICAL CLASSIFICATION

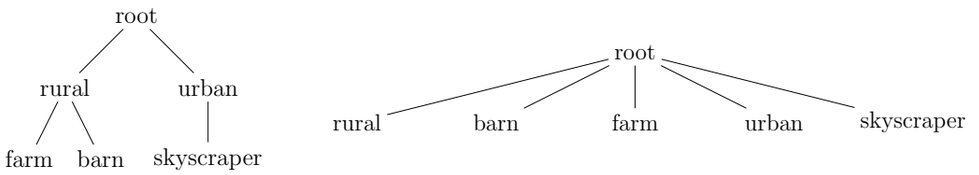


Figure 7.1: Hierarchical (left) and non-hierarchical (right) classification schemes. Barns and farms are common in rural areas, while skyscrapers are generally located in cities. While this relation can be clearly observed in the hierarchical model scheme, the connection is missing in the non-hierarchical design.

■

In multilabel classification, both the prediction $\widehat{\mathcal{Y}} := g(\boldsymbol{x})$ and the true response $\mathcal{Y}$ are *subsets* of the label set $\{0, \ldots, c-1\}$. A reasonable metric is the so-called *exact match ratio*,

EXACT MATCH RATIO

defined as

$$\text{exact match ratio} = \frac{\sum_{i=1}^{n} \mathbb{1}\{\widehat{\mathcal{Y}}_i = \mathcal{Y}_i\}}{n}.$$

The exact match ratio is rather stringent, as it requires a full match. In order to consider partial correctness, the following metrics could be used instead.

- The *accuracy* is defined as the ratio of correctly predicted labels and the total number of predicted and actual labels. The formula is given by

$$\text{accuracy} = \frac{\sum_{i=1}^{n} |\mathcal{Y}_i \cap \widehat{\mathcal{Y}}_i|}{\sum_{i=1}^{n} |\mathcal{Y}_i \cup \widehat{\mathcal{Y}}_i|}.$$

- The *precision* is defined as the ratio of correctly predicted labels and the total number of predicted labels. Specifically,

$$\text{precision} = \frac{\sum_{i=1}^{n} |\mathcal{Y}_i \cap \widehat{\mathcal{Y}}_i|}{\sum_{i=1}^{n} |\widehat{\mathcal{Y}}_i|}. \tag{7.7}$$

- The *recall* is defined as the ratio of correctly predicted labels and the total number of actual labels. Specifically,

$$\text{recall} = \frac{\sum_{i=1}^{n} |\mathcal{Y}_i \cap \widehat{\mathcal{Y}}_i|}{\sum_{i=1}^{n} |\mathcal{Y}_i|}. \tag{7.8}$$

- The *Hamming loss* counts the average number of incorrect predictions for all classes, calculated as

$$\text{Hamming} = \frac{1}{n\,c} \sum_{i=1}^{n} \sum_{y=0}^{c-1} \mathbb{1}\{y \in \widehat{\mathcal{Y}}_i\}\, \mathbb{1}\{y \notin \mathcal{Y}_i\} + \mathbb{1}\{y \notin \widehat{\mathcal{Y}}_i\}\, \mathbb{1}\{y \in \mathcal{Y}_i\}.$$

7.3 Classification via Bayes' Rule

We saw from Theorem 7.1 that the optimal classifier for classes $0, \ldots, c-1$ divides the feature space into c regions, depending on $f(y \mid \boldsymbol{x})$: the conditional pdf of the response Y given the feature vector $\boldsymbol{X} = \boldsymbol{x}$. In particular, if $f(y \mid \boldsymbol{x}) > f(z \mid \boldsymbol{x})$ for all $z \neq y$, the feature vector $\boldsymbol{x}$ is classified as y. Classifying feature vectors on the basis of their conditional class probabilities is a natural thing to do, especially in a Bayesian learning context; see Section 2.9 for an overview of Bayesian terminology and usage. Specifically, the conditional probability $f(y \mid \boldsymbol{x})$ is interpreted as a *posterior* probability, of the form

☞ 47

$$f(y \mid \boldsymbol{x}) \propto f(\boldsymbol{x} \mid y) f(y), \tag{7.9}$$

where $f(\boldsymbol{x} \mid y)$ is the *likelihood* of obtaining feature vector $\boldsymbol{x}$ from class y and $f(y)$ is the *prior* probability[1] of class y. By making various modeling assumptions about the prior

[1] Here we have used the Bayesian notation convention of "overloading" the notation f.

(e.g., all classes are *a priori* equally likely) and the likelihood function, one obtains the posterior pdf via Bayes' formula (7.9). A class $\widehat{y}$ is then assigned to a feature vector $\boldsymbol{x}$ according to the highest posterior probability; that is, we classify according to the *Bayes optimal decision rule*:

BAYES OPTIMAL DECISION RULE

$$\widehat{y} = \operatorname*{argmax}_y f(y \,|\, \boldsymbol{x}), \tag{7.10}$$

which is exactly (7.2). Since the discrete density $f(y \,|\, \boldsymbol{x})$, $y = 0, \ldots, c-1$ is usually not known, the aim is to approximate it well with a function $g(y \,|\, \boldsymbol{x})$ from some class of functions $\mathcal{G}$. Note that in this context, $g(\cdot \,|\, \boldsymbol{x})$ refers to a discrete density (a probability mass function) for a given $\boldsymbol{x}$.

Suppose a feature vector $\boldsymbol{x} = [x_1, \ldots, x_p]^\top$ of p features has to be classified into one of the classes $0, \ldots, c-1$. For example, the classes could be different people and the features could be various facial measurements, such as the width of the eyes divided by the distance between the eyes, or the ratio of the nose height and mouth width. In the *naïve Bayes* method, the class of approximating functions $\mathcal{G}$ is chosen such that $g(\boldsymbol{x} \,|\, y) = g(x_1 \,|\, y) \cdots g(x_p \,|\, y)$, that is, conditional on the label, all features are independent. Assuming a uniform prior for y, the posterior pdf can thus be written as

NAÏVE BAYES

$$g(y \,|\, \boldsymbol{x}) \propto \prod_{j=1}^{p} g(x_j \,|\, y),$$

where the marginal pdfs $g(x_j \,|\, y)$, $j = 1, \ldots, p$ belong to a given class of approximating functions $\mathcal{G}$. To classify $\boldsymbol{x}$, simply take the y that maximizes the unnormalized posterior pdf.

For instance, suppose that the approximating class $\mathcal{G}$ is such that $(X_j \,|\, y) \sim \mathcal{N}(\mu_{yj}, \sigma^2)$, $y = 0, \ldots, c-1$, $j = 1, \ldots, p$. The corresponding posterior pdf is then

$$g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x}) \propto \exp\left(-\frac{1}{2}\sum_{j=1}^{p}\frac{(x_j - \mu_{yj})^2}{\sigma^2}\right) = \exp\left(-\frac{1}{2}\frac{\|\boldsymbol{x} - \boldsymbol{\mu}_y\|^2}{\sigma^2}\right),$$

where $\boldsymbol{\mu}_y := [\mu_{y1}, \ldots, \mu_{yp}]^\top$ and $\boldsymbol{\theta} := \{\boldsymbol{\mu}_0, \ldots, \boldsymbol{\mu}_{c-1}, \sigma^2\}$ collects all model parameters. The probability $g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x})$ is maximal when $\|\boldsymbol{x} - \boldsymbol{\mu}_y\|$ is minimal. Thus $\widehat{y} = \operatorname{argmin}_y \|\boldsymbol{x} - \boldsymbol{\mu}_y\|$ is the classifier that maximizes the posterior probability. That is, classify $\boldsymbol{x}$ as y when $\boldsymbol{\mu}_y$ is closest to $\boldsymbol{x}$ in Euclidean distance. Of course, the parameters (here, the $\{\boldsymbol{\mu}_y\}$ and σ^2) are unknown and have to be estimated from the training data.

We can extend the above idea to the case where also the variance σ^2 depends on the class y and feature j, as in the next example.

■ **Example 7.1 (Naïve Bayes Classification)** Table 7.5 lists the means μ and standard deviations σ of $p = 3$ normally distributed features, for $c = 4$ different classes. How should a feature vector $\boldsymbol{x} = [1.67, 2.00, 4.23]^\top$ be classified? The posterior pdf is

$$g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x}) \propto (\sigma_{y1}\sigma_{y2}\sigma_{y3})^{-1} \exp\left(-\frac{1}{2}\sum_{j=1}^{3}\frac{(x_j - \mu_{yj})^2}{\sigma_{yj}^2}\right),$$

where $\boldsymbol{\theta} := \{\boldsymbol{\sigma}_j, \boldsymbol{\mu}_j\}_{j=0}^{c-1}$ again collects all model parameters. The (unscaled) values for $g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x})$, $y = 0, 1, 2, 3$ are 53.5, 0.24, 8.37, and 3.5×10^{-6}, respectively. Hence, the feature vector should be classified as 0. The code follows.

Table 7.5: Feature parameters.

	Feature 1		Feature 2		Feature 3	
Class	μ	σ	μ	σ	μ	σ
0	1.6	0.1	2.4	0.5	4.3	0.2
1	1.5	0.2	2.9	0.6	6.1	0.9
2	1.8	0.3	2.5	0.3	4.2	0.3
3	1.1	0.2	3.1	0.7	5.6	0.3

naiveBayes.py

```
import numpy as np
x = np.array([1.67,2,4.23]).reshape(1,3)
mu = np.array([1.6, 2.4, 4.3,
               1.5, 2.9, 6.1,
               1.8, 2.5, 4.2,
               1.1, 3.1, 5.6]).reshape(4,3)
sig = np.array([0.1, 0.5, 0.2,
                0.2, 0.6, 0.9,
                0.3, 0.3, 0.3,
                0.2, 0.7, 0.3]).reshape(4,3)
g = lambda y: 1/np.prod(sig[y,:]) * np.exp(
      -0.5*np.sum((x-mu[y,:])**2/sig[y,:]**2));
for y in range(0,4):
    print('{:3.2e}'.format(g(y)))
```

```
5.35e+01
2.42e-01
8.37e+00
3.53e-06
```

7.4 Linear and Quadratic Discriminant Analysis

The Bayesian viewpoint for classification of the previous section (not limited to naïve Bayes) leads in a natural way to the well-established technique of *discriminant analysis*. We discuss the binary classification case first, with classes 0 and 1.

DISCRIMINANT ANALYSIS

We consider a class of approximating functions $\mathcal{G}$ such that, conditional on the class $y \in \{0, 1\}$, the feature vector $\boldsymbol{X} = [X_1, \ldots, X_p]^\top$ has a $\mathcal{N}(\boldsymbol{\mu}_y, \boldsymbol{\Sigma}_y)$ distribution (see (2.33)):

☞ 45

$$g(\boldsymbol{x} \,|\, \boldsymbol{\theta}, y) = \frac{1}{\sqrt{(2\pi)^p \, |\boldsymbol{\Sigma}_y|}} \, \mathrm{e}^{-\frac{1}{2} (\boldsymbol{x}-\boldsymbol{\mu}_y)^\top \boldsymbol{\Sigma}_y^{-1} (\boldsymbol{x}-\boldsymbol{\mu}_y)}, \quad \boldsymbol{x} \in \mathbb{R}^p, \quad y \in \{0, 1\}, \tag{7.11}$$

where $\boldsymbol{\theta} = \{\alpha_j, \boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j\}_{j=0}^{c-1}$ collects all model parameters, including the probability vector $\boldsymbol{\alpha}$ (that is, $\sum_i \alpha_i = 1$ and $\alpha_i \geqslant 0$) which helps define the prior density: $g(y \,|\, \boldsymbol{\theta}) = \alpha_y, \; y \in \{0, 1\}$. Then, the posterior density is

$$g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x}) \propto \alpha_y \times g(\boldsymbol{x} \,|\, \boldsymbol{\theta}, y),$$

and, according to the Bayes optimal decision rule (7.10), we classify $\boldsymbol{x}$ to come from class 0 if $\alpha_0 g(\boldsymbol{x} \mid \boldsymbol{\theta}, 0) > \alpha_1 g(\boldsymbol{x} \mid \boldsymbol{\theta}, 1)$ or, equivalently (by taking logarithms) if,

$$\ln \alpha_0 - \frac{1}{2} \ln |\boldsymbol{\Sigma}_0| - \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu}_0)^\top \boldsymbol{\Sigma}_0^{-1}(\boldsymbol{x} - \boldsymbol{\mu}_0) > \ln \alpha_1 - \frac{1}{2} \ln |\boldsymbol{\Sigma}_1| - \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu}_1)^\top \boldsymbol{\Sigma}_1^{-1}(\boldsymbol{x} - \boldsymbol{\mu}_1).$$

The function

$$\delta_y(\boldsymbol{x}) = \ln \alpha_y - \frac{1}{2} \ln |\boldsymbol{\Sigma}_y| - \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu}_y)^\top \boldsymbol{\Sigma}_y^{-1}(\boldsymbol{x} - \boldsymbol{\mu}_y), \quad \boldsymbol{x} \in \mathbb{R}^p \tag{7.12}$$

QUADRATIC DISCRIMINANT FUNCTION

is called the *quadratic discriminant function* for class $y = 0, 1$. A point $\boldsymbol{x}$ is classified to class y for which $\delta_y(\boldsymbol{x})$ is largest. The function is quadratic in $\boldsymbol{x}$ and so the decision boundary $\{\boldsymbol{x} \in \mathbb{R}^p : \delta_0(\boldsymbol{x}) = \delta_1(\boldsymbol{x})\}$ is quadratic as well. An important simplification arises for the case where the assumption is made that $\boldsymbol{\Sigma}_0 = \boldsymbol{\Sigma}_1 = \boldsymbol{\Sigma}$. Now, the decision boundary is the set of $\boldsymbol{x}$ for which

$$\ln \alpha_0 - \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu}_0)^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{x} - \boldsymbol{\mu}_0) = \ln \alpha_1 - \frac{1}{2}(\boldsymbol{x} - \boldsymbol{\mu}_1)^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{x} - \boldsymbol{\mu}_1).$$

Expanding the above expression shows that the quadratic term in $\boldsymbol{x}$ is eliminated, giving a *linear* decision boundary in $\boldsymbol{x}$:

$$\ln \alpha_0 - \frac{1}{2}\boldsymbol{\mu}_0^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_0 + \boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_0 = \ln \alpha_1 - \frac{1}{2}\boldsymbol{\mu}_1^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_1 + \boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_1.$$

LINEAR DISCRIMINANT FUNCTION

The corresponding *linear discriminant function* for class y is

$$\delta_y(\boldsymbol{x}) = \ln \alpha_y - \frac{1}{2}\boldsymbol{\mu}_y^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_y + \boldsymbol{x}^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_y, \quad \boldsymbol{x} \in \mathbb{R}^p. \tag{7.13}$$

■ **Example 7.2 (Linear Discriminant Analysis)** Consider the case where $\alpha_0 = \alpha_1 = 1/2$ and

$$\boldsymbol{\Sigma} = \begin{bmatrix} 2 & 0.7 \\ 0.7 & 2 \end{bmatrix}, \quad \boldsymbol{\mu}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \boldsymbol{\mu}_1 = \begin{bmatrix} 2 \\ 4 \end{bmatrix}.$$

☞ 135

The distribution of $\boldsymbol{X}$ is a mixture of two bivariate normal distributions. Its pdf,

$$\frac{1}{2} g(\boldsymbol{x} \mid \boldsymbol{\theta}, y = 0) + \frac{1}{2} g(\boldsymbol{x} \mid \boldsymbol{\theta}, y = 1),$$

is depicted in Figure 7.2.

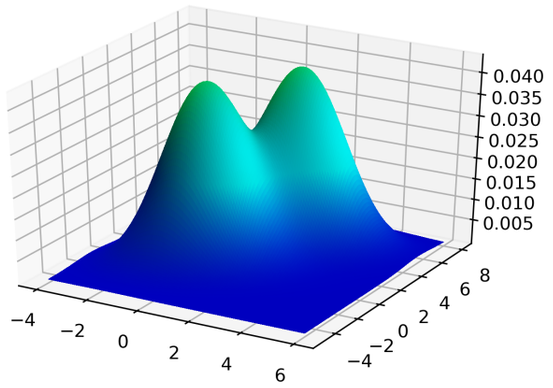


Figure 7.2: A Gaussian mixture density where the two mixture components have the same covariance matrix.

We used the following Python code to make this figure.

LDAmixture.py

```
import numpy as np, matplotlib.pyplot as plt
from scipy.stats import multivariate_normal
from mpl_toolkits.mplot3d import Axes3D
from matplotlib.colors import LightSource

mu0, mu1 = np.array([0,0]), np.array([2,4])
Sigma = np.array([[2,0.7],[0.7, 2]])
x, y = np.mgrid[-4:6:150j,-5:8:150j]
mvn0 = multivariate_normal( mu0, Sigma )
mvn1 = multivariate_normal( mu1, Sigma )

xy = np.hstack((x.reshape(-1,1),y.reshape(-1,1)))
z = 0.5*mvn0.pdf(xy).reshape(x.shape) +  0.5*mvn1.pdf(xy).reshape(x.
    shape)

fig = plt.figure()
ax = fig.gca(projection='3d')
ls = LightSource(azdeg=180, altdeg=65)
cols = ls.shade(z, plt.cm.winter)
surf = ax.plot_surface(x, y, z, rstride=1, cstride=1, linewidth=0,
                       antialiased=False, facecolors=cols)
plt.show()
```

The following Python code, which imports the previous code, draws a contour plot of the mixture density, simulates 1000 data points from the mixture density, and draws the decision boundary. To compute and display the linear decision boundary, let $[a_1, a_2]^\top = 2\boldsymbol{\Sigma}^{-1}(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0)$ and $b = \boldsymbol{\mu}_0^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_0 - \boldsymbol{\mu}_1^\top \boldsymbol{\Sigma}^{-1}\boldsymbol{\mu}_1$. Then, the decision boundary can be written as $a_1 x_1 + a_2 x_2 + b = 0$ or, equivalently, $x_2 = -(a_1 x_1 + b)/a_2$. We see in Figure 7.3 that the decision boundary nicely separates the two modes of the mixture density.

LDA.py

```
from LDAmixture import *
from numpy.random import rand
from numpy.linalg import inv

fig = plt.figure()
plt.contourf(x, y,z, cmap=plt.cm.Blues, alpha= 0.9,extend='both')
plt.ylim(-5.0,8.0)
plt.xlim(-4.0,6.0)
M = 1000
r = (rand(M,1) < 0.5)
for i in range(0,M):
    if r[i]:
       u = np.random.multivariate_normal(mu0,Sigma,1)
       plt.plot(u[0][0],u[0][1],'.r',alpha = 0.4)
    else:
       u = np.random.multivariate_normal(mu1,Sigma,1)
       plt.plot(u[0][0],u[0][1],'+k',alpha = 0.6)
```

```
a = 2*inv(Sigma) @ (mu1-mu0);
b = ( mu0.reshape(1,2) @ inv(Sigma) @ mu0.reshape(2,1)
    - mu1.reshape(1,2) @ inv(Sigma) @mu1.reshape(2,1) )
xx = np.linspace(-4,6,100)
yy = (-(a[0]*xx +b)/a[1])[0]
plt.plot(xx,yy,'m')
plt.show()
```

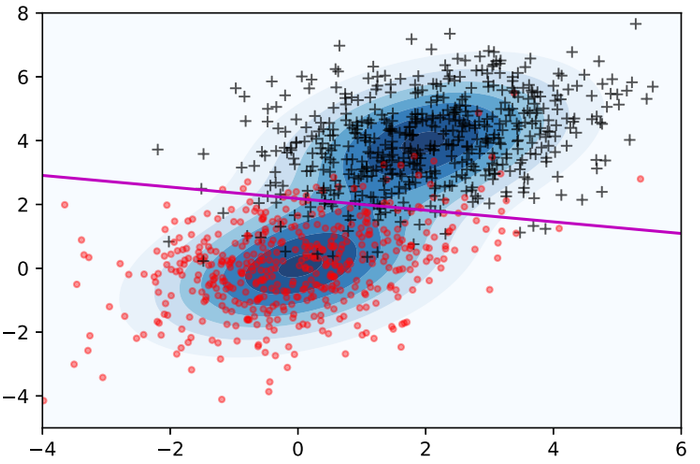


Figure 7.3: The linear discriminant boundary lies between the two modes of the mixture density and is linear.

■

To illustrate the difference between the linear and quadratic case, we specify different covariance matrices for the mixture components in the next example.

■ **Example 7.3 (Quadratic Discriminant Analysis)** As in Example 7.2 we consider a mixture of two Gaussians, but now with different covariance matrices. Figure 7.4 shows the quadratic decision boundary. The Python code follows.

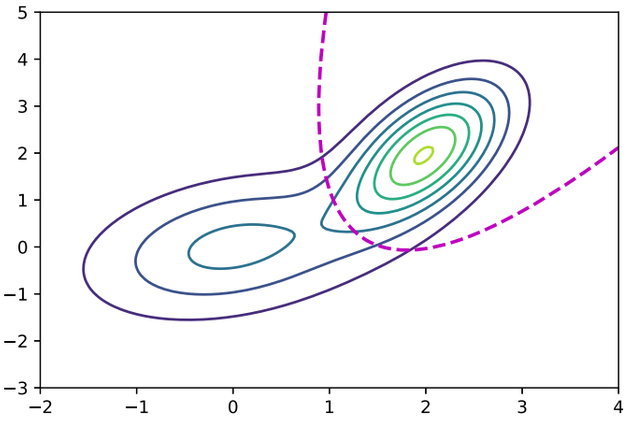


Figure 7.4: A quadratic decision boundary.

QDA.py

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import multivariate_normal

mu1 = np.array([0,0])
mu2 = np.array([2,2])
Sigma1 = np.array([[1,0.3],[0.3, 1]])
Sigma2 = np.array([[0.3,0.3],[0.3, 1]])
x, y = np.mgrid[-2:4:150j,-3:5:150j]
mvn1 = multivariate_normal( mu1, Sigma1 )
mvn2 = multivariate_normal( mu2, Sigma2 )

xy = np.hstack((x.reshape(-1,1),y.reshape(-1,1)))
z = ( 0.5*mvn1.pdf(xy).reshape(x.shape) +
      0.5*mvn2.pdf(xy).reshape(x.shape) )
plt.contour(x,y,z)

z1 = ( 0.5*mvn1.pdf(xy).reshape(x.shape) -
       0.5*mvn2.pdf(xy).reshape(x.shape))
plt.contour(x,y,z1, levels=[0],linestyles ='dashed',
            linewidths = 2, colors = 'm')
plt.show()
```

Of course, in practice the true parameter $\boldsymbol{\theta} = \{\alpha_j, \boldsymbol{\Sigma}_j, \boldsymbol{\mu}_j\}_{j=1}^c$ is not known and must be estimated from the training data — for example, by minimizing the *cross-entropy training loss* (4.4) with respect to $\boldsymbol{\theta}$: ☞ 123

$$\frac{1}{n}\sum_{i=1}^{n} \text{Loss}(f(\boldsymbol{x}_i, y_i), g(\boldsymbol{x}_i, y_i \,|\, \boldsymbol{\theta})) = -\frac{1}{n}\sum_{i=1}^{n} \ln g(\boldsymbol{x}_i, y_i \,|\, \boldsymbol{\theta}),$$

where

$$\ln g(\boldsymbol{x}, y \,|\, \boldsymbol{\theta}) = \ln \alpha_y - \frac{1}{2}\ln|\boldsymbol{\Sigma}_y| - \frac{1}{2}(\boldsymbol{x}-\boldsymbol{\mu}_y)^\top \boldsymbol{\Sigma}_y^{-1}(\boldsymbol{x}-\boldsymbol{\mu}_y) - \frac{p}{2}\ln(2\pi).$$

The corresponding estimates of the model parameters (see Exercise 2) are:

$$\begin{aligned} \widehat{\alpha}_y &= \frac{n_y}{n} \\ \widehat{\boldsymbol{\mu}}_y &= \frac{1}{n_y}\sum_{i:y_i=y} \boldsymbol{x}_i \\ \widehat{\boldsymbol{\Sigma}}_y &= \frac{1}{n_y}\sum_{i:y_i=y} (\boldsymbol{x}_i - \widehat{\boldsymbol{\mu}}_y)(\boldsymbol{x}_i - \widehat{\boldsymbol{\mu}}_y)^\top \end{aligned} \tag{7.14}$$

for $y = 0, \ldots, c-1$, where $n_y := \sum_{i=1}^n \mathbb{1}\{y_i = y\}$. For the case where $\boldsymbol{\Sigma}_y = \boldsymbol{\Sigma}$ for all y, we have $\widehat{\boldsymbol{\Sigma}} = \sum_y \widehat{\alpha}_y \widehat{\boldsymbol{\Sigma}}_y$.

When $c > 2$ classes are involved, the classification procedure carries through in exactly the same way, leading to quadratic and linear discriminant functions (7.12) and (7.13) for each class. The space $\mathbb{R}^p$ now is partitioned into c regions, determined by the linear or quadratic boundaries determined by each pair of Gaussians.

SPHERE THE DATA

For the linear discriminant case (that is, when $\boldsymbol{\Sigma}_y = \boldsymbol{\Sigma}$ for all y), it is convenient to first "whiten" or *sphere the data* as follows. Let $\mathbf{B}$ be an invertible matrix such that $\boldsymbol{\Sigma} = \mathbf{B}\mathbf{B}^\top$, obtained, for example, via the Cholesky method. We linearly transform each data point $\boldsymbol{x}$ to $\boldsymbol{x}' := \mathbf{B}^{-1}\boldsymbol{x}$ and each mean $\boldsymbol{\mu}_y$ to $\boldsymbol{\mu}'_y := \mathbf{B}^{-1}\boldsymbol{\mu}_y$, $y = 0, \ldots, c-1$. Let the random vector $\boldsymbol{X}$ be distributed according to the mixture pdf

☞ 375

$$g_X(\boldsymbol{x} \,|\, \boldsymbol{\theta}) := \sum_y \alpha_y \, \frac{1}{\sqrt{(2\pi)^p \, |\boldsymbol{\Sigma}_y|}} \, \mathrm{e}^{-\frac{1}{2}\,(\boldsymbol{x}-\boldsymbol{\mu}_y)^\top \boldsymbol{\Sigma}_y^{-1} (\boldsymbol{x}-\boldsymbol{\mu}_y)}.$$

☞ 435

Then, by the transformation Theorem C.4, the vector $\boldsymbol{X}' = \mathbf{B}^{-1}\boldsymbol{X}$ has density

$$\begin{aligned} g_{X'}(\boldsymbol{x}' \,|\, \boldsymbol{\theta}) &= \frac{g_X(\boldsymbol{x} \,|\, \boldsymbol{\theta})}{|\mathbf{B}^{-1}|} = \sum_{y=0}^{c-1} \frac{\alpha_y}{\sqrt{(2\pi)^p}} \, \mathrm{e}^{-\frac{1}{2}\,(\boldsymbol{x}-\boldsymbol{\mu}_y)^\top (\mathbf{B}\mathbf{B}^\top)^{-1} (\boldsymbol{x}-\boldsymbol{\mu}_y)} \\ &= \sum_{y=0}^{c-1} \frac{\alpha_y}{\sqrt{(2\pi)^p}} \, \mathrm{e}^{-\frac{1}{2}\,(\boldsymbol{x}'-\boldsymbol{\mu}'_y)^\top (\boldsymbol{x}'-\boldsymbol{\mu}'_y)} = \sum_{y=0}^{c-1} \frac{\alpha_y}{\sqrt{(2\pi)^p}} \, \mathrm{e}^{-\frac{1}{2}\,\|\boldsymbol{x}'-\boldsymbol{\mu}'_y\|^2}. \end{aligned}$$

This is the pdf of a mixture of standard p-dimensional normal distributions. The name "sphering" derives from the fact that the contours of each mixture component are perfect spheres. Classification of the transformed data is now particularly easy: classify $\boldsymbol{x}$ as $\widehat{y} := \operatorname{argmin}_y \{ \|\boldsymbol{x}' - \boldsymbol{\mu}'_y\|^2 - 2 \ln \alpha_y \}$. Note that this rule only depends on the prior probabilities and the distance from $\boldsymbol{x}'$ to the transformed means $\{\boldsymbol{\mu}'_y\}$. This procedure can lead to a significant dimensionality reduction of the data. Namely, the data can be projected onto the space spanned by the differences between the mean vectors $\{\boldsymbol{\mu}'_y\}$. When there are c classes, this is a $(c-1)$-dimensional space, as opposed to the p-dimensional space of the original data. We explain the precise ideas via an example.

■ **Example 7.4 (Classification after Data Reduction)** Consider an equal mixture of three 3-dimensional Gaussian distributions with identical covariance matrices. After sphering the data, the covariance matrices are all equal to the identity matrix. Suppose the mean vectors of the sphered data are $\boldsymbol{\mu}_1 = [2, 1, -3]^\top$, $\boldsymbol{\mu}_2 = [1, -4, 0]^\top$, and $\boldsymbol{\mu}_3 = [2, 4, 6]^\top$. The left panel of Figure 7.5 shows the 3-dimensional (sphered) data from each of the three classes.

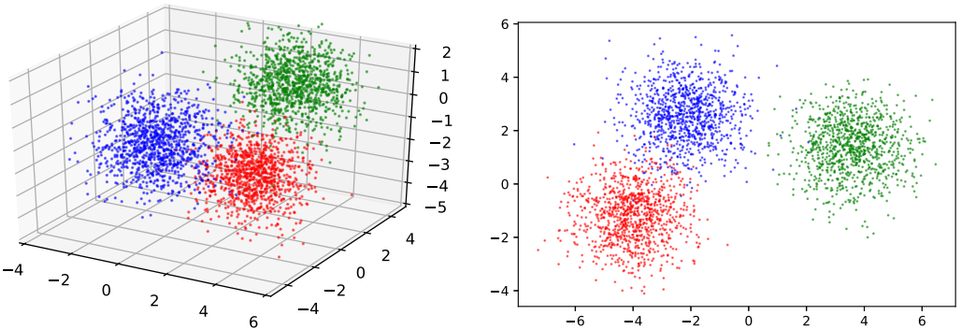


Figure 7.5: Left: original data. Right: projected data.

The data are stored in three 1000×3 matrices $\mathbf{X}_1$, $\mathbf{X}_2$, and $\mathbf{X}_3$. Here is how the data was generated and plotted.

datared.py

```
import numpy as np
from numpy.random import randn
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D

n=1000
mu1 = np.array([2,1,-3])
mu2 = np.array([1,-4,0])
mu3 = np.array([2,4,0])
X1 = randn(n,3) + mu1
X2 = randn(n,3) + mu2
X3 = randn(n,3) + mu3
fig = plt.figure()
ax = fig.gca(projection='3d',)
ax.plot(X1[:,0],X1[:,1],X1[:,2],'r.',alpha=0.5,markersize=2)
ax.plot(X2[:,0],X2[:,1],X2[:,2],'b.',alpha=0.5,markersize=2)
ax.plot(X3[:,0],X3[:,1],X3[:,2],'g.',alpha=0.5,markersize=2)
ax.set_xlim3d(-4,6)
ax.set_ylim3d(-5,5)
ax.set_zlim3d(-5,2)
plt.show()
```

Since we have equal mixtures, we classify each data point $\boldsymbol{x}$ according to the closest distance to $\boldsymbol{\mu}_1$, $\boldsymbol{\mu}_2$, or $\boldsymbol{\mu}_3$. We can achieve a reduction in the dimensionality of the data by *projecting* the data onto the two-dimensional affine space spanned by the $\{\boldsymbol{\mu}_i\}$; that is, all vectors are of the form

$$\boldsymbol{\mu}_1 + \beta_1(\boldsymbol{\mu}_2 - \boldsymbol{\mu}_1) + \beta_2(\boldsymbol{\mu}_3 - \boldsymbol{\mu}_1), \quad \beta_1, \beta_2 \in \mathbb{R}.$$

In fact, one may just as well project the data onto the subspace spanned by the vectors $\boldsymbol{\mu}_{21} = \boldsymbol{\mu}_2 - \boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_{31} = \boldsymbol{\mu}_3 - \boldsymbol{\mu}_1$. Let $\mathbf{W} = [\boldsymbol{\mu}_{21}, \boldsymbol{\mu}_{31}]$ be the 3×2 matrix whose columns are $\boldsymbol{\mu}_{21}$ and $\boldsymbol{\mu}_{31}$. The orthogonal projection matrix onto the subspace $\mathcal{W}$ spanned by the columns of $\mathbf{W}$ is (see Theorem A.4): ☞ 364

$$\mathbf{P} = \mathbf{W}\mathbf{W}^+ = \mathbf{W}(\mathbf{W}^\top \mathbf{W})^{-1}\mathbf{W}^\top.$$

Let $\mathbf{U}\mathbf{D}\mathbf{V}^\top$ be the singular value decomposition of $\mathbf{W}$. Then $\mathbf{P}$ can also be written as

$$\mathbf{P} = \mathbf{U}\mathbf{D}(\mathbf{D}^\top \mathbf{D})^{-1}\mathbf{D}^\top \mathbf{U}^\top.$$

Note that $\mathbf{D}$ has dimension 3×2, so is not square. The first two columns of $\mathbf{U}$, say $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$, form an orthonormal basis of the subspace $\mathcal{W}$. What we want to do is rotate this subspace to the $x-y$ plane, mapping $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ to $[1,0,0]^\top$ and $[0,1,0]^\top$, respectively. This is achieved via the rotation matrix $\mathbf{U}^{-1} = \mathbf{U}^\top$, giving the skewed projection matrix

$$\mathbf{R} = \mathbf{U}^\top \mathbf{P} = \mathbf{D}(\mathbf{D}^\top \mathbf{D})^{-1}\mathbf{D}^\top \mathbf{U}^\top,$$

whose 3rd row only contains zeros. Applying $\mathbf{R}$ to all the data points, and ignoring the 3rd component of the projected points (which is 0), gives the right panel of Figure 7.5. We see that the projected points are much better separated than the original ones. We have achieved dimensionality reduction of the data while retaining all the necessary information required for classification. Here is the rest of the Python code.

dataproj.py

```
from datared import *
from numpy.linalg import svd, pinv
mu21 = (mu2 - mu1).reshape(3,1)
mu31 = (mu3 - mu1).reshape(3,1)
W = np.hstack((mu21, mu31))
U,_,_ = svd(W)  # we only need U
P = W @ pinv(W)
R = U.T @ P

RX1 = (R @ X1.T).T
RX2 = (R @ X2.T).T
RX3 = (R @ X3.T).T
plt.plot(RX1[:,0],RX1[:,1],'b.',alpha=0.5,markersize=2)
plt.plot(RX2[:,0],RX2[:,1],'g.',alpha=0.5,markersize=2)
plt.plot(RX3[:,0],RX3[:,1],'r.',alpha=0.5,markersize=2)
plt.show()
```

7.5 Logistic Regression and Softmax Classification

☞ 204

In Example 5.10 we introduced the logistic (logit) regression model as a generalized linear model where, conditional on a p-dimensonal feature vector $\boldsymbol{x}$, the random response Y has a $\mathsf{Ber}(h(\boldsymbol{x}^\top\boldsymbol{\beta}))$ distribution with $h(u) = 1/(1+\mathrm{e}^{-u})$. The parameter $\boldsymbol{\beta}$ was then learned from the training data by maximizing the likelihood of the training responses or, equivalently,

☞ 123

by minimizing the supervised version of the *cross-entropy training loss* (4.4):

$$-\frac{1}{n}\sum_{i=1}^{n} \ln g(y_i \,|\, \boldsymbol{\beta}, \boldsymbol{x}_i),$$

where $g(y=1\,|\,\boldsymbol{\beta},\boldsymbol{x}) = 1/(1+\mathrm{e}^{-\boldsymbol{x}^\top\boldsymbol{\beta}})$ and $g(y=0\,|\,\boldsymbol{\beta},\boldsymbol{x}) = \mathrm{e}^{-\boldsymbol{x}^\top\boldsymbol{\beta}}/(1+\mathrm{e}^{-\boldsymbol{x}^\top\boldsymbol{\beta}})$. In particular, we have

$$\ln \frac{g(y=1\,|\,\boldsymbol{\beta},\boldsymbol{x})}{g(y=0\,|\,\boldsymbol{\beta},\boldsymbol{x})} = \boldsymbol{x}^\top\boldsymbol{\beta}. \tag{7.15}$$

LOG-ODDS RATIO

In other words, the *log-odds ratio* is a linear function of the feature vector. As a consequence, the decision boundary $\{\boldsymbol{x} : g(y=0\,|\,\boldsymbol{\beta},\boldsymbol{x}) = g(y=1\,|\,\boldsymbol{\beta},\boldsymbol{x})\}$ is the hyperplane $\boldsymbol{x}^\top\boldsymbol{\beta} = 0$. Note that $\boldsymbol{x}$ typically includes the constant feature. If the constant feature is considered separately, that is $\boldsymbol{x} = [1, \widetilde{\boldsymbol{x}}^\top]^\top$, then the boundary is an affine hyperplane in $\widetilde{\boldsymbol{x}}$.

Suppose that training on $\tau = \{(\boldsymbol{x}_i, y_i)\}$ yields the estimate $\widehat{\boldsymbol{\beta}}$ with the corresponding learner $g_\tau(y=1\,|\,\boldsymbol{x}) = 1/(1+\mathrm{e}^{-\boldsymbol{x}^\top\widehat{\boldsymbol{\beta}}})$. The learner can be used as a pre-classifier from which we obtain the classifier $\mathbb{1}\{g_\tau(y=1\,|\,\boldsymbol{x}) > 1/2\}$ or, equivalently,

$$\widehat{y} := \operatorname*{argmax}_{j\in\{0,1\}} g_\tau(y=j\,|\,\boldsymbol{x}),$$

in accordance with the fundamental classification rule (7.2).

The above classification methodology for the logit model can be generalized to the

MULTI-LOGIT

multi-logit model where the response takes values in the set $\{0,\ldots,c-1\}$. The key idea is

to replace (7.15) with

$$\ln \frac{g(y=j\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x})}{g(y=0\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x})} = \boldsymbol{x}^\top \boldsymbol{\beta}_j, \quad j=1,\ldots,c-1, \tag{7.16}$$

where the matrix $\mathbf{W} \in \mathbb{R}^{(c-1)\times(p-1)}$ and vector $\boldsymbol{b} \in \mathbb{R}^{c-1}$ reparameterize all $\boldsymbol{\beta}_j \in \mathbb{R}^p$ such that (recall $\boldsymbol{x} = [1, \widetilde{\boldsymbol{x}}^\top]^\top$):

$$\mathbf{W}\widetilde{\boldsymbol{x}} + \boldsymbol{b} = [\boldsymbol{\beta}_1,\ldots,\boldsymbol{\beta}_{c-1}]^\top \boldsymbol{x}.$$

Observe that the random response Y is assumed to have a conditional probability distribution for which the log-odds ratio with respect to class j and a "reference" class (in this case 0) is *linear*. The separating boundaries between two pairs of classes are again affine hyperplanes.

The model (7.16) completely specifies the distribution of Y, namely:

$$g(y\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x}) = \frac{\exp(z_{y+1})}{\sum_{k=1}^{c}\exp(z_k)}, \quad y=0,\ldots,c-1,$$

where z_1 is an arbitrary constant, say 0, corresponding to the "reference" class $y=0$, and

$$[z_2,\ldots,z_c]^\top := \mathbf{W}\widetilde{\boldsymbol{x}} + \boldsymbol{b}.$$

Note that $g(y\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x})$ is the $(y+1)$-st component of $\boldsymbol{a} = \operatorname{softmax}(\boldsymbol{z})$, where

$$\operatorname{softmax} : \boldsymbol{z} \mapsto \frac{\exp(\boldsymbol{z})}{\sum_k \exp(z_k)}$$

is the *softmax* function and $\boldsymbol{z} = [z_1,\ldots,z_c]^\top$. Finally, we can write the classifier as SOFTMAX

$$\widehat{y} = \operatorname*{argmax}_{j\in\{0,\ldots,c-1\}} a_{j+1}.$$

In summary, we have the sequence of mappings transforming the input $\boldsymbol{x}$ into the output $\widehat{y}$:

$$\boldsymbol{x} \to \mathbf{W}\widetilde{\boldsymbol{x}} + \boldsymbol{b} \to \operatorname{softmax}(\boldsymbol{z}) \to \operatorname*{argmax}_{j\in\{0,\ldots,c-1\}} a_{j+1} \to \widehat{y}.$$

In Example 9.4 we will revisit the multi-logit model and reinterpret this sequence of mappings as a *neural network*. In the context of neural networks, $\mathbf{W}$ is called a *weight* matrix and $\boldsymbol{b}$ is called a *bias* vector. ☞ 335

The parameters $\mathbf{W}$ and $\boldsymbol{b}$ have to be learned from the training data, which involves minimization of the supervised version of the *cross-entropy training loss* (4.4): ☞ 123

$$\frac{1}{n}\sum_{i=1}^{n} \operatorname{Loss}(f(y_i\,|\,\boldsymbol{x}_i), g(y_i\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x}_i)) = -\frac{1}{n}\sum_{i=1}^{n} \ln g(y_i\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x}_i).$$

Using the softmax function, the *cross-entropy* loss can be simplified to:

$$\operatorname{Loss}(f(y\,|\,\boldsymbol{x}), g(y\,|\,\mathbf{W},\boldsymbol{b},\boldsymbol{x})) = -z_{y+1} + \ln\sum_{k=1}^{c}\exp(z_k). \tag{7.17}$$

The discussion on training is postponed until Chapter 9, where we reinterpret the multi-logit model as a neural net, which can be trained using the *limited-memory BFGS* method (Exercise 11). Note that in the binary case ($c=2$), where there is only one vector $\boldsymbol{\beta}$ to be estimated, Example 5.10 already established that minimization of the cross-entropy training loss is equivalent to likelihood maximization. ☞ 354

7.6 K-Nearest Neighbors Classification

Let $\tau = \{(\boldsymbol{x}_i, y_i)\}_{i=1}^n$ be the training set, with $y_i \in \{0, \ldots, c-1\}$, and let $\boldsymbol{x}$ be a new feature vector. Define $\boldsymbol{x}_{(1)}, \boldsymbol{x}_{(2)}, \ldots, \boldsymbol{x}_{(n)}$ as the feature vectors ordered by closeness to $\boldsymbol{x}$ in some distance $\text{dist}(\boldsymbol{x}, \boldsymbol{x}_i)$, e.g., the Euclidean distance $\|\boldsymbol{x}-\boldsymbol{x}'\|$. Let $\tau(\boldsymbol{x}) := \{(\boldsymbol{x}_{(1)}, y_{(1)}) \ldots, (\boldsymbol{x}_{(K)}, y_{(K)})\}$ be the subset of τ that contains K feature vectors $\boldsymbol{x}_i$ that are closest to $\boldsymbol{x}$. Then the *K-nearest neighbors* classification rule classifies $\boldsymbol{x}$ according to the most frequently occurring class labels in $\tau(\boldsymbol{x})$. If two or more labels receive the same number of votes, the feature vector is classified by selecting one of these labels randomly with equal probability. For the case $K = 1$ the set $\tau(\boldsymbol{x})$ contains only one element, say $(\boldsymbol{x}', y')$, and $\boldsymbol{x}$ is classified as y'. This divides the space into n regions

K-NEAREST NEIGHBORS

$$\mathcal{R}_i = \{\boldsymbol{x} : \text{dist}(\boldsymbol{x}, \boldsymbol{x}_i) \leqslant \text{dist}(\boldsymbol{x}, \boldsymbol{x}_j),\ j \neq i\}, \quad i = 1, \ldots, n.$$

For a feature space $\mathbb{R}^p$ with the Euclidean distance, this gives a Voronoi tessellation of the feature space, similar to what was done for vector quantization in Section 4.6.

☞ 142

■ **Example 7.5 (Nearest Neighbor Classification)** The Python program below simulates 80 random points above and below the line $x_2 = x_1$. Points above the line $x_2 = x_1$ have label 0 and points below this line have label 1. Figure 7.6 shows the Voronoi tessellation obtained from the 1-nearest neighbor classification.

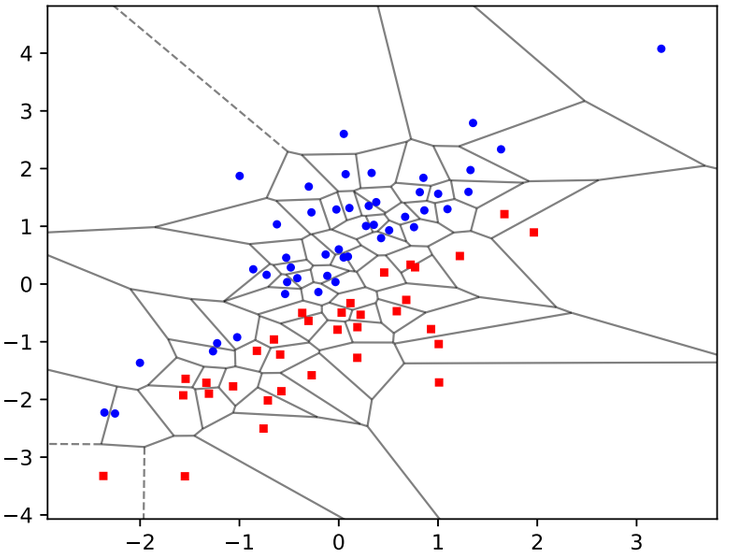


Figure 7.6: The 1-nearest neighbor algorithm divides up the space into Voronoi cells.

nearestnb.py

```
import numpy as np
from numpy.random import rand,randn
import matplotlib.pyplot as plt
from scipy.spatial import Voronoi, voronoi_plot_2d
```

```
np.random.seed(12345)
M = 80
x = randn(M,2)
y = np.zeros(M) # pre-allocate list

for i in range(M):
    if rand()<0.5:
        x[i,1], y[i] = x[i,0] + np.abs(randn()), 0
    else:
        x[i,1], y[i] = x[i,0] - np.abs(randn()), 1

vor = Voronoi(x)
plt_options = {'show_vertices':False, 'show_points':False,
               'line_alpha':0.5}
fig = voronoi_plot_2d(vor, **plt_options)
plt.plot(x[y==0,0], x[y==0,1],'bo',
         x[y==1,0], x[y==1,1],'rs', markersize=3)
```

7.7 Support Vector Machine

Suppose we are given the training set $\tau = \{(\boldsymbol{x}_i, y_i)\}_{i=1}^n$, where each response[2] y_i takes either the value -1 or 1, and we wish to construct a classifier taking values in $\{-1, 1\}$. As this merely involves a relabeling of the 0–1 classification problem in Section 7.1, the optimal classification function for the indicator loss, $\mathbb{1}\{y \neq \widehat{y}\}$, is, by Theorem 7.1, equal to

$$g^*(\boldsymbol{x}) = \begin{cases} 1 & \text{if} \quad \mathbb{P}[Y = 1 \,|\, \boldsymbol{X} = \boldsymbol{x}] \geqslant 1/2, \\ -1 & \text{if} \quad \mathbb{P}[Y = 1 \,|\, \boldsymbol{X} = \boldsymbol{x}] < 1/2. \end{cases}$$

It is not difficult to show, see Exercise 5, that the function g^* can be viewed as the minimizer of the risk for the *hinge loss* function, $\text{Loss}(y, \widehat{y}) = (1 - y\widehat{y})_+ := \max\{0,\ 1 - y\widehat{y}\}$, over all prediction functions g (not necessarily taking values only in the set $\{-1, 1\}$). That is,

HINGE LOSS

$$g^* = \operatorname*{argmin}_g \mathbb{E}\,(1 - Y\, g(\boldsymbol{X}))_+. \tag{7.18}$$

Given the training set τ, we can approximate the risk $\ell(g) = \mathbb{E}\,(1 - Y\, g(\boldsymbol{X}))_+$ with the training loss

$$\ell_\tau(g) = \frac{1}{n} \sum_{i=1}^n (1 - y_i\, g(\boldsymbol{x}_i))_+,$$

and minimize this over a (smaller) class of functions to obtain the optimal prediction function g_τ. Finally, as the prediction function g_τ generally is not a classifier by itself (it usually does not only take values -1 or 1), we take the classifier

$$\text{sign}\, g_\tau(\boldsymbol{x}).$$

[2] The reason why we use responses -1 and 1 here, instead of 0 and 1, is that the notation becomes easier.

OPTIMAL DECISION BOUNDARY

Therefore, a feature vector $\boldsymbol{x}$ is classified according to 1 or -1 depending on whether $g_\tau(\boldsymbol{x}) \geqslant 0$ or < 0, respectively. The *optimal decision boundary* is given by the set of $\boldsymbol{x}$ for which $g_\tau(\boldsymbol{x}) = 0$.

Similar to the cubic smoothing spline or RKHS setting in (6.19), we can consider finding the best classifier, given the training data, via the penalized goodness-of-fit optimization:

$$\min_{g \in \mathcal{H} \oplus \mathcal{H}_0} \frac{1}{n} \sum_{i=1}^{n} [1 - y_i \, g(\boldsymbol{x}_i)]_+ + \widetilde{\gamma} \, \|g\|_{\mathcal{H}}^2,$$

for some regularization parameter $\widetilde{\gamma}$. It will be convenient to define $\gamma := 2n\widetilde{\gamma}$ and to solve the equivalent problem

$$\min_{g \in \mathcal{H} \oplus \mathcal{H}_0} \sum_{i=1}^{n} [1 - y_i \, g(\boldsymbol{x}_i)]_+ + \frac{\gamma}{2} \, \|g\|_{\mathcal{H}}^2.$$

☞ 232 We know from the Representer Theorem 6.6 that if κ is the reproducing kernel corresponding to $\mathcal{H}$, then the solution is of the form (assuming that the null space $\mathcal{H}_0$ has a constant term only):

$$g(\boldsymbol{x}) = \alpha_0 + \sum_{i=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}). \tag{7.19}$$

☞ 232 Substituting into the minimization expression yields the analogue of (6.21):

$$\min_{\boldsymbol{\alpha}, \alpha_0} \sum_{i=1}^{n} [1 - y_i(\alpha_0 + \{\mathbf{K}\boldsymbol{\alpha}\}_i)]_+ + \frac{\gamma}{2} \, \boldsymbol{\alpha}^\top \mathbf{K} \boldsymbol{\alpha}, \tag{7.20}$$

where $\mathbf{K}$ is the Gram matrix. This is a *convex* optimization problem, as it is the sum of a convex quadratic and piecewise linear term in $\boldsymbol{\alpha}$. Defining $\lambda_i := \gamma \alpha_i / y_i$, $i = 1, \ldots, n$ and $\boldsymbol{\lambda} := [\lambda_1, \ldots, \lambda_n]^\top$, we show in Exercise 10 that the optimal $\boldsymbol{\alpha}$ and α_0 in (7.20) can be obtained by solving the "dual" convex optimization problem

$$\begin{aligned} \max_{\boldsymbol{\lambda}} \quad & \sum_{i=1}^{n} \lambda_i - \frac{1}{2\gamma} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j y_i y_j \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) \\ \text{subject to:} \quad & \boldsymbol{\lambda}^\top \boldsymbol{y} = 0, \; \mathbf{0} \leqslant \boldsymbol{\lambda} \leqslant \mathbf{1}, \end{aligned} \tag{7.21}$$

and $\alpha_0 = y_j - \sum_{i=1} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j)$ for any j for which $\lambda_j \in (0, 1)$. In view of (7.19), the optimal prediction function (pre-classifier) g_τ is then given by

$$g_\tau(\boldsymbol{x}) = \alpha_0 + \sum_{i=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}) = \alpha_0 + \frac{1}{\gamma} \sum_{i=1}^{n} y_i \lambda_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}). \tag{7.22}$$

To mitigate possible numerical problems in the calculation of α_0 it is customary to take an overall average:

$$\alpha_0 = \frac{1}{|\mathcal{J}|} \sum_{j \in \mathcal{J}} \left\{ y_j - \sum_{i=1}^{n} \alpha_i \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) \right\},$$

where $\mathcal{J} := \{j : \lambda_j \in (0, 1)\}$.

Note that, from (7.22), the optimal pre-classifier $g(\boldsymbol{x})$ and the classifier sign $g(\boldsymbol{x})$ only depend on vectors $\boldsymbol{x}_i$ for which $\lambda_i \neq 0$. These vectors are called the *support vectors* of the support vector machine. It is also important to note that the quadratic function in (7.21) depends on the regularization parameter γ. By defining $\nu_i := \lambda_i/\gamma$, $i = 1, \ldots, n$, we can rewrite (7.21) as

SUPPORT VECTORS

$$\begin{aligned} \min_{\boldsymbol{\nu}} \quad & \frac{1}{2} \sum_{i,j} \nu_i \nu_j y_i y_j \, \kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) - \sum_{i=1}^{n} \nu_i \\ \text{subject to:} \quad & \sum_{i=1}^{n} \nu_i y_i = 0, \;\; 0 \leqslant \nu_i \leqslant 1/\gamma =: C, \quad i = 1, \ldots, n. \end{aligned} \tag{7.23}$$

For perfectly separable data, that is, data for which an affine plane can be drawn to perfectly separate the two classes, we may take $C = \infty$, as explained below. Otherwise, C needs to be chosen via cross-validation or a test data set, for example.

Geometric interpretation

For the linear kernel function $\kappa(\boldsymbol{x}, \boldsymbol{x}') = \boldsymbol{x}^\top \boldsymbol{x}'$, we have

$$g_\tau(\boldsymbol{x}) = \beta_0 + \boldsymbol{\beta}^\top \boldsymbol{x},$$

with $\beta_0 = \alpha_0$ and $\boldsymbol{\beta} = \gamma^{-1} \sum_{i=1}^n \lambda_i y_i \boldsymbol{x}_i = \sum_{i=1}^n \alpha_i \boldsymbol{x}_i$, and so the decision boundary is an affine plane. The situation is illustrated in Figure 7.7. The decision boundary is formed by the points $\boldsymbol{x}$ such that $g_\tau(\boldsymbol{x}) = 0$. The two sets $\{\boldsymbol{x} : g_\tau(\boldsymbol{x}) = -1\}$ and $\{\boldsymbol{x} : g_\tau(\boldsymbol{x}) = 1\}$ are called the *margins*. The distance from the points on a margin to the decision boundary is $1/\|\boldsymbol{\beta}\|$.

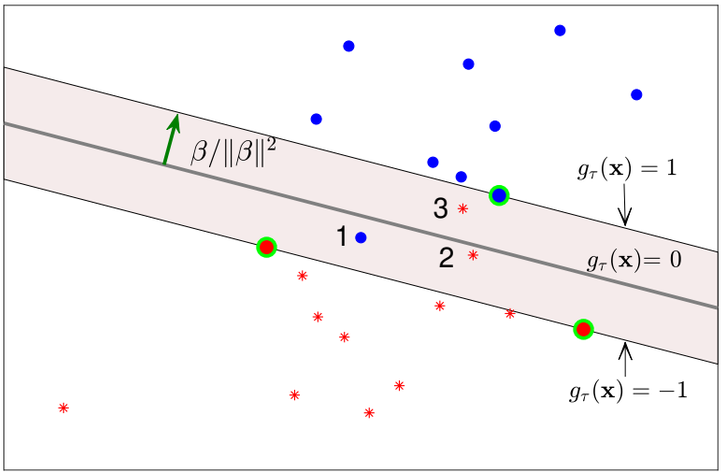


Figure 7.7: Classifying two classes (red and blue) using SVM.

Based on the "multipliers" $\{\lambda_i\}$, we can divide the training samples $\{(\boldsymbol{x}_i, y_i)\}$ into three categories (see Exercise 11):

- Points for which $\lambda_i \in (0, 1)$. These are the support vectors on the margins (green encircled in the figure) and are correctly classified.

- Points for which $\lambda_i = 1$. These points, which are also support vectors, lie strictly inside the margins (points 1, 2, and 3 in the figure). Such points may or may not be correctly classified.

- Points for which $\lambda_i = 0$. These are the non-support vectors, which all lie outside the margins. Every such point is correctly classified.

If the classes of points $\{\boldsymbol{x}_i : y_i = 1\}$ and $\{\boldsymbol{x}_i : y_i = -1\}$ are perfectly separable by some affine plane, then there will be no points strictly inside the margins, so all support vectors will lie exactly on the margins. In this case (7.20) reduces to

$$\begin{aligned} &\min_{\boldsymbol{\beta},\beta_0} \ \|\boldsymbol{\beta}\|^2 \\ &\text{subject to:} \quad y_i(\beta_0 + \boldsymbol{x}_i^\top \boldsymbol{\beta}) \geqslant 1, \ i = 1, \ldots, n, \end{aligned} \tag{7.24}$$

using the fact that $\alpha_0 = \beta_0$ and $\mathbf{K}\boldsymbol{\alpha} = \mathbf{X}\mathbf{X}^\top\boldsymbol{\alpha} = \mathbf{X}\boldsymbol{\beta}$. We may replace $\min \|\boldsymbol{\beta}\|^2$ in (7.24) with $\max 1/\|\boldsymbol{\beta}\|$, as this gives the same optimal solution. As $1/\|\boldsymbol{\beta}\|$ is equal to half the margin width, the latter optimization problem has a simple interpretation: separate the points via an affine hyperplane such that the margin width is maximized.

■ **Example 7.6 (Support Vector Machine)** The data in Figure 7.8 was uniformly generated on the unit disc. Class-1 points (blue dots) have a radius less than 1/2 (y-values 1) and class-2 points (red crosses) have a radius greater than 1/2 (y-values -1).

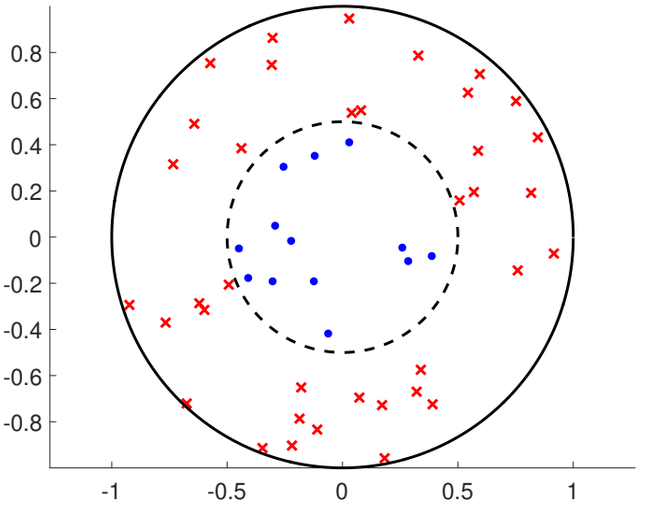


Figure 7.8: Separate the two classes.

Of course it is not possible to separate the two groups of points via a straight line in $\mathbb{R}^2$. However, it is possible to separate them in $\mathbb{R}^3$ by considering three-dimensional feature vectors $\boldsymbol{z} = [z_1, z_2, z_3]^\top = [x_1, x_2, x_1^2 + x_2^2]^\top$. For any $\boldsymbol{x} \in \mathbb{R}^2$, the corresponding feature vector $\boldsymbol{z}$ lies on a quadratic surface. In this space it is possible to separate the $\{\boldsymbol{z}_i\}$ points into two groups by means of a planar surface, as illustrated in Figure 7.9.

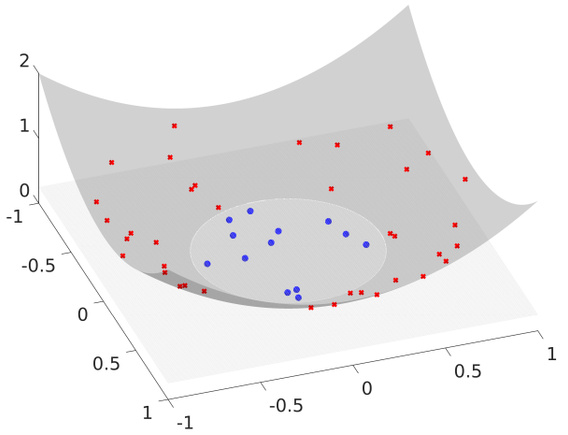


Figure 7.9: In feature space $\mathbb{R}^3$ the points can be separated by a plane.

We wish to find a separating plane in $\mathbb{R}^3$ using the transformed features. The following Python code uses the **SVC** function of the **sklearn** module to solve the quadratic optimization problem (7.23) (with $C = \infty$). The results are summarized in Table 7.6. The data is available from the book's GitHub site as `svmcirc.csv`.

svmquad.py

```
import numpy as np
from numpy import genfromtxt
from sklearn.svm import SVC

data = genfromtxt('svmcirc.csv', delimiter=',')
x = data[:,[0,1]] #vectors are rows
y = data[:,[2]].reshape(len(x),) #labels

tmp = np.sum(np.power(x,2),axis=1).reshape(len(x),1)
z = np.hstack((x,tmp))

clf = SVC(C = np.inf, kernel='linear')
clf.fit(z,y)

print("Support Vectors \n", clf.support_vectors_)
print("Support Vector Labels ",y[clf.support_])
print("Nu",clf.dual_coef_)
print("Bias",clf.intercept_)
```

```
  Support Vectors
 [[ 0.038758    0.53796     0.29090314]
 [-0.49116    -0.20563     0.28352184]
 [-0.45068    -0.04797     0.20541358]
 [-0.061107   -0.41651     0.17721465]]
Support Vector Labels  [-1. -1.  1.  1.]
Nu [[ -46.49249413 -249.01807328  265.31805855   30.19250886]]
Bias  [5.617891]
```

Table 7.6: Optimal support vector machine parameters for the $\mathbb{R}^3$ data.

$z^\top$			y	$\alpha = \nu y$
0.0388	0.5380	0.2909	−1	−46.4925
−0.4912	−0.2056	0.2835	−1	−249.0181
−0.4507	−0.0480	0.2054	1	265.3181
−0.0611	−0.4165	0.1772	1	30.1925

It follows that the normal vector of the plane is

$$\boldsymbol{\beta} = \sum_{i \in \mathcal{S}} \alpha_i \boldsymbol{z}_i = [-0.9128, 0.8917, -24.2764]^\top,$$

where $\mathcal{S}$ is the set of indices of the support vectors. We see that the plane is almost perpendicular to the z_1, z_2 plane. The bias term β_0 can also be found from the table above. In particular, for any $\boldsymbol{x}^\top$ and y in Table 7.6, we have $y - \boldsymbol{\beta}^\top \boldsymbol{z} = \beta_0 = 5.6179$.

To draw the separating boundary in $\mathbb{R}^2$ we need to project the intersection of the separating plane with the quadratic surface onto the z_1, z_2 plane. That is, we need to find all points (z_1, z_2) such that

$$5.6179 - 0.9128 z_1 + 0.8917 z_2 = 24.2764\,(z_1^2 + z_2^2). \tag{7.25}$$

This is the equation of a circle with (approximate) center $(0.019, -0.018)$ and radius 0.48, which is very close to the true circular boundary between the two groups, with center $(0, 0)$ and radius 0.5. This circle is drawn in Figure 7.10.

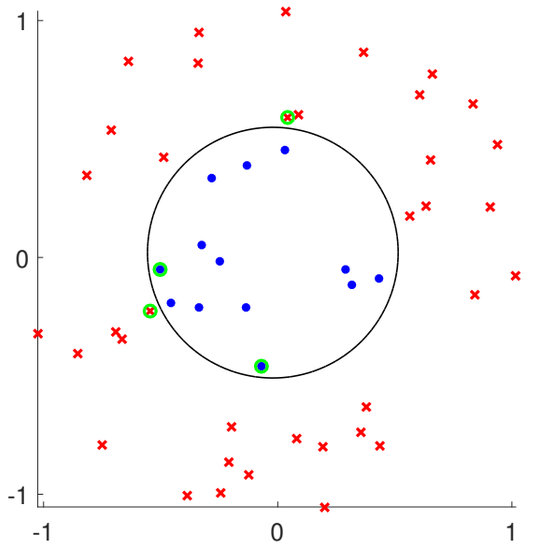


Figure 7.10: The circular decision boundary can be viewed equivalently as (a) the projection onto the x_1, x_2 plane of the intersection of the separating plane with the quadratic surface (both in $\mathbb{R}^3$), or (b) the set of points $\boldsymbol{x} = (x_1, x_2)$ for which $g_\tau(\boldsymbol{x}) = \beta_0 + \boldsymbol{\beta}^\top \boldsymbol{\phi}(\boldsymbol{x}) = 0$.

An equivalent way to derive this circular separating boundary is to consider the feature map $\boldsymbol{\phi}(\boldsymbol{x}) = [x_1, x_2, x_1^2 + x_2^2]^\top$ on $\mathbb{R}^2$, which defines a reproducing kernel

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = \boldsymbol{\phi}(\boldsymbol{x})^\top \boldsymbol{\phi}(\boldsymbol{x}'),$$

on $\mathbb{R}^2$, which in turn gives rise to a (unique) RKHS $\mathcal{H}$. The optimal prediction function (7.19) is now of the form

$$g_\tau(\boldsymbol{x}) = \alpha_0 + \frac{1}{\gamma}\sum_{i=1}^{n} y_i\,\lambda_i\,\boldsymbol{\phi}(\boldsymbol{x}_i)^\top\boldsymbol{\phi}(\boldsymbol{x}) = \beta_0 + \boldsymbol{\beta}^\top\boldsymbol{\phi}(\boldsymbol{x}), \tag{7.26}$$

where $\alpha_0 = \beta_0$ and

$$\boldsymbol{\beta} = \frac{1}{\gamma}\sum_{i=1}^{n} y_i\,\lambda_i\,\boldsymbol{\phi}(\boldsymbol{x}_i).$$

The decision boundary, $\{\boldsymbol{x} : g_\tau(\boldsymbol{x}) = 0\}$, is again a circle in $\mathbb{R}^2$. The following code determines the fitted model parameters and the decision boundary. Figure 7.10 shows the optimal decision boundary, which is identical to (7.25). The function **mykernel** specifies the custom kernel above.

svmkern.py

```
import numpy as np, matplotlib.pyplot as plt
from numpy import genfromtxt
from sklearn.svm import SVC

def mykernel(U,V):
    tmpU = np.sum(np.power(U,2),axis=1).reshape(len(U),1)
    U = np.hstack((U,tmpU))
    tmpV = np.sum(np.power(V,2),axis=1).reshape(len(V),1)
    V = np.hstack((V,tmpV))
    K = U @ V.T
    print(K.shape)
    return K

# read in the data
inp = genfromtxt('svmcirc.csv', delimiter=',')
data = inp[:,[0,1]] #vectors are rows
y = inp[:,[2]].reshape(len(data),) #labels

clf = SVC(C = np.inf, kernel=mykernel, gamma='auto') # custom kernel
# clf = SVC(C = np.inf, kernel="rbf", gamma='scale') # inbuilt

clf.fit(data,y)

print("Support Vectors \n", clf.support_vectors_)
print("Support Vector Labels ",y[clf.support_])
print("Nu ",clf.dual_coef_)
print("Bias ",clf.intercept_)

# plot
d = 0.001
x_min, x_max = -1,1
y_min, y_max = -1,1
xx, yy = np.meshgrid(np.arange(x_min, x_max, d), np.arange(y_min,
    y_max, d))
plt.plot(data[clf.support_,0],data[clf.support_,1],'go')
plt.plot(data[y==1,0],data[y==1,1],'b.')
plt.plot(data[y==-1,0],data[y==-1,1],'rx')
```

```
Z = clf.predict(np.c_[xx.ravel(), yy.ravel()])
Z = Z.reshape(xx.shape)
plt.contour(xx, yy, Z,colors ="k")
plt.show()
```

Finally, we illustrate the use of the Gaussian kernel

$$\kappa(\boldsymbol{x}, \boldsymbol{x}') = \mathrm{e}^{-c\,\|\boldsymbol{x}-\boldsymbol{x}'\|^2}, \tag{7.27}$$

where $c > 0$ is some tuning constant. This is an example of a *radial basis function kernel*, which are reproducing kernels of the form $\kappa(\boldsymbol{x}, \boldsymbol{x}') = f(\|\boldsymbol{x} - \boldsymbol{x}'\|)$, for some positive real-valued function f. Each feature vector $\boldsymbol{x}$ is now transformed to a *function* $\kappa_{\boldsymbol{x}} = \kappa(\boldsymbol{x}, \cdot)$. We can think of it as the (unnormalized) pdf of a Gaussian distribution centered around $\boldsymbol{x}$, and g_τ is a (signed) *mixture* of these pdfs, plus a constant; that is,

$$g_\tau(\boldsymbol{x}) = \alpha_0 + \sum_{i=1}^{n} \alpha_i \, \mathrm{e}^{-c\,\|\boldsymbol{x}_i-\boldsymbol{x}\|^2}.$$

Replacing in Line 2 of the previous code `mykernel` with `'rbf'` produces the SVM parameters given in Table 7.7. Figure 7.11 shows the decision boundary, which is not exactly circular, but is close to the true (circular) boundary $\{\boldsymbol{x} : \|\boldsymbol{x}\| = 1/2\}$. There are now seven support vectors, rather than the four in Figure 7.10.

Table 7.7: Optimal support vector machine parameters for the Gaussian kernel case.

$\boldsymbol{x}^\top$		y	α ($\times 10^9$)	$\boldsymbol{x}^\top$		y	α ($\times 10^9$)
0.0388	0.5380	−1	−0.0635	−0.4374	0.3854	−1	−1.4399
−0.4912	−0.2056	−1	−9.4793	0.3402	−0.5740	−1	−0.1000
0.5086	0.1576	−1	−0.5240	−0.4098	−0.1763	1	6.0662
−0.4507	−0.0480	1	5.5405				

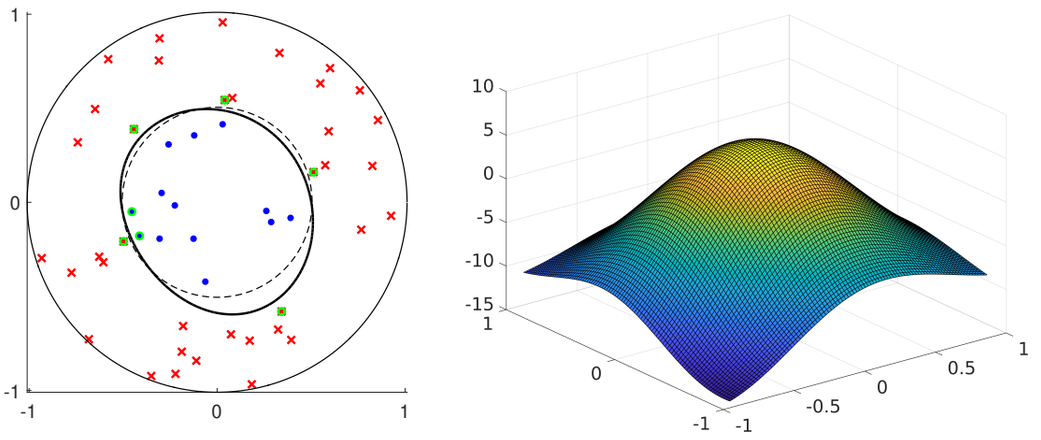


Figure 7.11: Left: The decision boundary $\{\boldsymbol{x} : g_\tau(\boldsymbol{x}) = 0\}$ is roughly circular, and separates the two classes well. There are seven support vectors, indicated by green circles. Right: The graph of g_τ is a scaled mixture of Gaussian pdfs plus a constant.

■ **Remark 7.2 (Scaling and Penalty Parameters)** When using a radial basis function in `SVC` in `sklearn`, the scaling c (7.27) can be set via the parameter `gamma`. Note that large values of `gamma` lead to highly peaked predicted functions, and small values lead to highly smoothed predicted functions. The parameter `C` in `SVC` refers $C = 1/\gamma$ in (7.23). ■

7.8 Classification with Scikit-Learn

In this section we apply several classification methods to a real-world data set, using the Python module `sklearn` (the package name is Scikit-Learn). Specifically, the data is obtained from UCI's Breast Cancer Wisconsin data set. This data set, first published and analyzed in [118], contains the measurements related to 569 images of 357 benign and 212 malignant breast masses. The goal is to classify a breast mass as benign or malignant based on 10 features: Radius, Texture, Perimeter, Area, Smoothness, Compactness, Concavity, Concave Points, Symmetry, and Fractal Dimension of each mass. The mean, standard error, and "worst" of these attributes were computed for each image, resulting in 30 features. For instance, feature 1 is Mean Radius, feature 11 is Radius SE, feature 21 is Worst Radius.

The following Python code reads the data, extracts the response vector and model (feature) matrix and divides the data into a training and test set.

skclass1.py

```
from numpy import genfromtxt
from sklearn.model_selection import train_test_split
url1 = "http://mlr.cs.umass.edu/ml/machine-learning-databases/"
url2 = "breast-cancer-wisconsin/"
name = "wdbc.data"
data = genfromtxt(url1 + url2 + name, delimiter=',', dtype=str)
y = data[:,1] #responses
X = data[:,2:].astype('float') #features as an ndarray matrix

X_train , X_test , y_train , y_test = train_test_split(
        X, y, test_size = 0.4, random_state = 1234)
```

To visualize the data we create a 3D scatterplot for the features mean *radius*, mean *texture*, and mean *concavity*, which correspond to the columns 0, 1, and 6 of the model matrix **X**. Figure 7.12 suggests that the malignant and benign breast masses could be well separated using these three features.

skclass2.py

```
from skclass1 import X, y
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D
import numpy as np

Bidx = np.where(y == 'B')
Midx= np.where(y == 'M')

# plot features Radius (column 0), Texture (1), Concavity (6)
```

```
fig = plt.figure()
ax = fig.gca(projection = '3d')
ax.scatter(X[Bidx,0], X[Bidx,1], X[Bidx,6],
           c='r', marker='^', label='Benign')
ax.scatter(X[Midx,0], X[Midx,1], X[Midx,6],
           c='b', marker='o', label='Malignant')
ax.legend()
ax.set_xlabel('Mean Radius')
ax.set_ylabel('Mean Texture')
ax.set_zlabel('Mean Concavity')
plt.show()
```

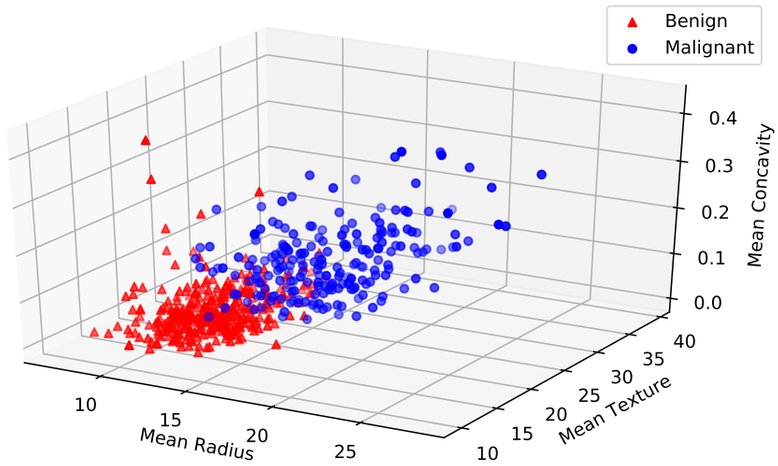


Figure 7.12: Scatterplot of three features of the benign and malignant breast masses.

The following code uses various classifiers to predict the category of breast masses (benign or malignant). In this case the training set has 341 elements and the test set has 228 elements. For each classifier the percentage of correct predictions (that is, the accuracy) in the test set is reported. We see that in this case quadratic discriminant analysis gives the highest accuracy (0.956). Exercise 18 explores the question whether this metric is the most appropriate for these data.

skclass3.py

```
from skclass1 import X_train, y_train, X_test, y_test
from sklearn.metrics import accuracy_score

import sklearn.discriminant_analysis as DA
from sklearn.naive_bayes import GaussianNB
from sklearn.neighbors import KNeighborsClassifier
from sklearn.linear_model import LogisticRegression
from sklearn.svm import SVC

names = ["Logit","NBayes", "LDA", "QDA", "KNN", "SVM"]
```

```
classifiers = [LogisticRegression(C=1e5),
               GaussianNB(),
               DA.LinearDiscriminantAnalysis(),
               DA.QuadraticDiscriminantAnalysis(),
               KNeighborsClassifier(n_neighbors=5),
               SVC(kernel='rbf', gamma = 1e-4)]

print('Name  Accuracy\n'+14*'-')
for name, clf in zip(names, classifiers):
  clf.fit(X_train, y_train)
  y_pred = clf.predict(X_test)
  print('{:6}  {:3.3f}'.format(name, accuracy_score(y_test,y_pred)))
```

```
Name  Accuracy
--------------
Logit   0.943
NBayes  0.908
LDA     0.943
QDA     0.956
KNN     0.925
SVM     0.939
```

Further Reading

An excellent source for understanding various pattern recognition techniques is the book [35] by Duda et al. Theoretical foundations of classification, including the Vapnik–Chernovenkis dimension and the fundamental theorem of learning, are discussed in [109, 121, 122]. A popular measure for characterizing the performance of a binary classifier is the *receiver operating characteristic* (ROC) curve [38]. The naïve Bayes classification paradigm can be extended to handle explanatory variable dependency via graphical models such as Bayesian networks and Markov random fields [46, 66, 69]. For a detailed discussion on Bayesian decision theory, see [8].

Exercises

1. Let $0 \leqslant w \leqslant 1$. Show that the solution to the convex optimization problem

$$\begin{aligned} &\min_{p_1,\ldots,p_n} \sum_{i=1}^{n} p_i^2 \\ &\text{subject to: } \sum_{i-1}^{n-1} p_i = w \text{ and } \sum_{i=1}^{n} p_i = 1, \end{aligned} \tag{7.28}$$

is given by $p_i = w/(n-1), i = 1, \ldots, n-1$ and $p_n = 1 - w$.

2. Derive the formulas (7.14) by minimizing the cross-entropy training loss:

$$-\frac{1}{n} \sum_{i=1}^{n} \ln g(\boldsymbol{x}_i, y_i \,|\, \boldsymbol{\theta}),$$

where $g(\boldsymbol{x}, y \,|\, \boldsymbol{\theta})$ is such that:

$$\ln g(\boldsymbol{x}, y \,|\, \boldsymbol{\theta}) = \ln \alpha_y - \frac{1}{2} \ln |\boldsymbol{\Sigma}_y| - \frac{1}{2} (\boldsymbol{x} - \boldsymbol{\mu}_y)^\top \boldsymbol{\Sigma}_y^{-1} (\boldsymbol{x} - \boldsymbol{\mu}_y) - \frac{p}{2} \ln(2\pi).$$

3. Adapt the code in Example 7.2 to plot the estimated decision boundary instead of the true one in Figure 7.3. Compare the true and estimated decision boundaries.

4. Recall from equation (7.16) that the decision boundaries of the multi-logit classifier are linear, and that the pre-classifier can be written as a conditional pdf of the form:

$$g(y \,|\, \mathbf{W}, \boldsymbol{b}, \boldsymbol{x}) = \frac{\exp(z_{y+1})}{\sum_{i=1}^{c} \exp(z_i)}, \quad y \in \{0, \ldots, c-1\},$$

where $\boldsymbol{x}^\top = [1, \widetilde{\boldsymbol{x}}^\top]$ and $\boldsymbol{z} = \mathbf{W}\widetilde{\boldsymbol{x}} + \boldsymbol{b}$.

(a) Show that the linear discriminant pre-classifier in Section 7.4 can also be written as a conditional pdf of the form ($\boldsymbol{\theta} = \{\alpha_y, \boldsymbol{\Sigma}_y, \boldsymbol{\mu}_y\}_{y=0}^{c-1}$):

$$g(y \,|\, \boldsymbol{\theta}, \boldsymbol{x}) = \frac{\exp(z_{y+1})}{\sum_{i=1}^{c} \exp(z_i)}, \quad y \in \{0, \ldots, c-1\},$$

where $\boldsymbol{x}^\top = [1, \widetilde{\boldsymbol{x}}^\top]$ and $\boldsymbol{z} = \mathbf{W}\widetilde{\boldsymbol{x}} + \boldsymbol{b}$. Find formulas for the corresponding $\boldsymbol{b}$ and $\mathbf{W}$ in terms of the linear discriminant parameters $\{\alpha_y, \boldsymbol{\mu}_y, \boldsymbol{\Sigma}_y\}_{y=0}^{c-1}$, where $\boldsymbol{\Sigma}_y = \boldsymbol{\Sigma}$ for all y.

(b) Explain which pre-classifier has smaller approximation error: the linear discriminant or multi-logit one? Justify your answer by proving an inequality between the two approximation errors.

5. Consider a binary classification problem where the response Y takes values in $\{-1, 1\}$. Show that optimal prediction function for the hinge loss $\text{Loss}(y, \widehat{y}) = (1 - y\widehat{y})_+ := \max\{0, 1 - y\widehat{y}\}$ is the same as the optimal prediction function g^* for the indicator loss:

$$g^*(\boldsymbol{x}) = \begin{cases} 1 & \text{if} \quad \mathbb{P}[Y = 1 \,|\, \boldsymbol{X} = \boldsymbol{x}] > 1/2, \\ -1 & \text{if} \quad \mathbb{P}[Y = 1 \,|\, \boldsymbol{X} = \boldsymbol{x}] < 1/2. \end{cases}$$

That is, show that

$$\mathbb{E}\,(1 - Y\, h(\boldsymbol{X}))_+ \geqslant \mathbb{E}\,(1 - Y\, g^*(\boldsymbol{X}))_+ \tag{7.29}$$

for all functions h.

☞ 158

6. In Example 4.12, we applied a principal component analysis (PCA) to the **iris** data, but refrained from classifying the flowers based on their feature vectors $\boldsymbol{x}$. Implement a 1-nearest neighbor algorithm, using a training set of 50 randomly chosen data pairs $(\boldsymbol{x}, y)$ from the **iris** data set. How many of the remaining 100 flowers are correctly classified? Now classify these entries with an off-the-shelf multi-logit classifier, e.g., such as can be found in the **sklearn** and **statsmodels** packages.

7. Figure 7.13 displays two groups of data points, given in Table 7.8. The convex hulls have also been plotted. It is possible to separate the two classes of points via a straight line.