Machine Learning in Astronomy

by

Lise du Buisson

Minor Dissertation presented in partial fulfilment of the requirements for the degree of Master of Science

in the
Department of Mathematics and Applied Mathematics
University of Cape Town

May 2015

Supervisor: Professor Bruce A. Bassett
The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.
Declaration of Authorship

I, Lise du Buisson, know the meaning of plagiarism and declare that all of the work in the dissertation titled “Machine Learning in Astronomy”, save for that which is properly acknowledged, is my own.

It should be noted that a paper entitled “Machine Learning Classification of SDSS Transient Survey Images” by du Buisson et al. [1], based on the work in this thesis, has been submitted to the Monthly Notices of the Royal Astronomical Society (MNRAS) journal. The current version of the paper can be found at http://arxiv.org/abs/1407.4118. Some sections from the paper have been modified for the purposes of using it in this thesis, and Figures 2.5, 3.6, 4.3, 5.1, 5.2, 5.3 and 5.4 as well as Tables 3.2, 5.1, 5.7, 5.9, 5.10, 5.11, 5.12 and C.1 have been produced both for use in the paper and this thesis, and so appear in both.

Signed: Signature removed

Date: 21 May 2015
“There are worlds out there where the sky is burning, and the sea’s asleep, and the rivers dream; people made of smoke and cities made of song. Somewhere there’s danger, somewhere there’s injustice, and somewhere else the tea’s getting cold. Come on, Ace. We’ve got work to do.”

The Seventh Doctor, Doctor Who
The search to find answers to the deepest questions we have about the Universe has fueled the collection of data for ever larger volumes of our cosmos. The field of supernova cosmology, for example, is seeing continuous development with upcoming surveys set to produce a vast amount of data that will require new statistical inference and machine learning techniques for processing and analysis. Distinguishing between real objects and artefacts is one of the first steps in any transient science pipeline and, currently, is still carried out by humans - often leading to hand scanners having to sort hundreds or thousands of images per night. This is a time-consuming activity introducing human biases that are extremely hard to characterise. To succeed in the objectives of future transient surveys, the successful substitution of human hand scanners with machine learning techniques for the purpose of this artefact-transient classification therefore represents a vital frontier. In this thesis we test various machine learning algorithms and show that many of them can match the human hand scanner performance in classifying transient difference $g$, $r$ and $i$-band imaging data from the SDSS-II SN Survey into real objects and artefacts. Using principal component analysis and linear discriminant analysis, we construct a grand total of 56 feature sets with which to train, optimise and test a Minimum Error Classifier (MEC), a na"ive Bayes classifier, a $k$-Nearest Neighbours (kNN) algorithm, a Support Vector Machine (SVM) and the SkyNet artificial neural network. We find that kNN is the best-performing classifier with an accuracy of 89% and a recall of 90%. Three of our classifiers (kNN, SkyNet and MEC) match the human recall performance of $\sim$ 96% on the fake SNe injected into the SDSS pipeline, accomplishing our goal. We also show that none of our best-performing classifiers are highly correlated in their classifications, an indication that an ensemble classifier might yield improved results. Extending this research by further making use of multiple epoch data, object histories and host galaxy information can lead to further improvements.
Acknowledgements

First and foremost, I thank my supervisor, Bruce Bassett - for readily providing me with advice and support whenever I was in need of it, and for setting a great example in both a personal and academic capacity. For making me look up and remember the bigger picture every once in a while - it sometimes does wonders to remember that soon we’ll all be dead and we should live our lives doing what we want and should to be happy.

I thoroughly enjoyed collaborating with Navin Sivanandam, “my” postdoc, who were always willing to lend a friendly hand when I needed explanations and who made the environment fun with his interesting and unique take on life. Thanks also to Mathew Smith, another collaborator, for valuable advice and for supplying the data for my project.

This year would have been a lot less fun without Michelle, with whom I successfully created one of the world’s most counter-productive office environments, and to whom I am extremely grateful for lending a kind ear in difficult times. My other office-mates, friends and colleagues gave AIMS the welcoming and warm character I will remember it by. They are Eli and Ermias (who had to put up with me and Michelle), Gilad, Kai, Rene, Mark and Iggy. Mika, Amidou and Ayman made long nights in the computer laboratory anything but tedious, and didn’t hesitate to make me feel at home during those first days of NASSP when I was a bit dazed and confused.

I would not have been able to complete my masters were it not for the love and support from a few other very important people. My mother and father, for their love and support for anything and everything I do; my brother, Johan, for his friendship and our honest discussions that I value so much, and for all the tea and coffee; Nathan, for being a true friend - whose discussions on life, liberty and the pursuit of happiness always left me feeling free of all chains, and who braved the early morning traffic back to Stellenbosch many times for me during those first months; Nadeem, who I journeyed with for a very special few years that I will always cherish. And then, Filipe, who made this last year truly remarkable. For standing by my side through the good times and the bad, for arranging surprise visits from the UK, for proof-reading my thesis without complaining, for introducing me to Doctor Who and for being the most perfect adventure companion that I could’ve asked for.
Formal Acknowledgements

I acknowledge funding from the Square Kilometre Array (SKA) Project and the National Research Foundation (NRF) for the duration of my postgraduate studies, and support and resources from the African Institute for Mathematical Sciences (AIMS). I further thank Johan A. du Preez and Ben Herbst for their insights during the initial phases of the project, and the University College London (UCL) Physics and Astronomy Department for the use of their computer cluster, Splinter.

Funding for the SDSS and SDSS-II has been provided by the Alfred P. Sloan Foundation, the Participating Institutions, the National Science Foundation, the U.S. Department of Energy, the National Aeronautics and Space Administration, the Japanese Monbukagakusho, the Max Planck Society, and the Higher Education Funding Council for England. The SDSS Web Site is http://www.sdss.org.

The SDSS is managed by the Astrophysical Research Consortium for the Participating Institutions. The Participating Institutions are the American Museum of Natural History, Astrophysical Institute Potsdam, University of Basel, Cambridge University, Case Western Reserve University, University of Chicago, Drexel University, Fermilab, the Institute for Advanced Study, the Japan Participation Group, Johns Hopkins University, the Joint Institute for Nuclear Astrophysics, the Kavli Institute for Particle Astrophysics and Cosmology, the Korean Scientist Group, the Chinese Academy of Sciences (LAMOST), Los Alamos National Laboratory, the Max-Planck-Institute for Astronomy (MPIA), the Max-Planck-Institute for Astrophysics (MPA), New Mexico State University, Ohio State University, University of Pittsburgh, University of Portsmouth, Princeton University, the United States Naval Observatory, and the University of Washington.
## Contents

Declaration of Authorship i

Abstract iii

Acknowledgements iv

List of Figures x

List of Tables xi

Abbreviations xii

Physical Constants xiii

1 The History of Machine Learning 1

1.1 Introduction ................................................. 1

1.2 AI and Machine Learning: A Modern History .................. 2

1.2.1 The Gestation Period (1943-1955) .......................... 2

1.2.2 The Dawn of Artificial Intelligence (1956) .................. 3

1.2.3 Early Days and Expectations (1952-1969) ................... 3

1.2.4 Reality Strikes (1966-1973) .............................. 4

1.2.5 Knowledge-Based Systems (1969-1979) and the AI Industry (1980-present) 5

1.2.6 The Rise of Machine Learning (1980-present) ............... 6

1.3 Machine Learning Applications in Astronomy ................. 8

1.3.1 Classification of Objects .................................. 8

1.3.2 Photometric Redshifts .................................... 9

1.3.3 Other Applications ....................................... 10

2 An Introduction to Machine Learning 11

2.1 Introduction ................................................. 11

2.1.1 Important Concepts ....................................... 11

2.1.2 Learning Categories ...................................... 13

2.1.2.1 Supervised Learning: Classification ................... 14

2.2 Machine Learning Algorithms ............................... 15

2.2.1 Naïve Bayes ............................................ 15
## Contents

2.2.1.1 Bayes Theorem: A Machine Learning Perspective ........................................ 15
2.2.1.2 The Naïve Bayes Classifier ................................................................. 17
2.2.2 k-Nearest Neighbours ............................................................ 18
    2.2.2.1 Remarks on the Algorithm ......................................................... 20
2.2.3 Support Vector Machine ............................................................ 21
    2.2.3.1 Formulation of the Support Vector Machine Algorithm ............. 21
    2.2.3.2 Kernel Functions ................................................................. 24
    2.2.3.3 Linearly Non-Separable Class Distributions ......................... 25
    2.2.3.4 Obtaining Probabilistic Outputs ............................................. 27
2.2.4 Artificial Neural Network ......................................................... 28
    2.2.4.1 The Perceptron ................................................................. 29
    2.2.4.2 Feed-Forward Neural Networks .............................................. 30
    2.2.4.3 Autoencoders ................................................................. 33
    2.2.4.4 Network Training ............................................................. 33
2.3 Feature Extraction ................................................................. 34
    2.3.1 Principal Component Analysis .................................................. 34
    2.3.1.1 Derivation of PCA – the Maximum Variance Formulation ......... 35
2.3.2 Linear Discriminant Analysis .................................................. 38
2.4 Concluding Remarks ............................................................... 41

3 Supernova Cosmology ................................................................. 42
    3.1 Introduction ................................................................. 42
3.2 Supernova Cosmology ............................................................... 42
    3.2.1 Distance Measurements .......................................................... 45
    3.2.2 Type Ia Supernovae as Standard Candles .............................. 47
    3.2.3 The Data Deluge ................................................................. 49
3.3 The Sloan Digital Sky Survey: Supernova Survey ........................................... 51
    3.3.1 The SDSS-II Supernova Survey ............................................... 51
    3.3.1.1 The Supernova Survey Science Goals ..................................... 52
    3.3.1.2 Technical aspects of the SN Survey ...................................... 53
3.4 Classification Goals and Chosen Dataset .................................................. 55
    3.4.1 Dataset and Classification Systems ....................................... 56
    3.4.2 Training and Testing Protocol ............................................... 56
    3.4.3 Layout of the Remainder of the Thesis ..................................... 58

4 Feature Extraction ................................................................. 61
    4.1 Introduction ................................................................. 61
4.2 Pre-Processing ................................................................. 62
4.3 Feature Extraction ............................................................... 62
    4.3.1 Principal Component Analysis ............................................... 63
    4.3.1.1 The Algorithm ............................................................... 64
    4.3.1.2 Creating the Input Vectors .............................................. 65
    4.3.1.3 Multi-class PCA ............................................................. 66
    4.3.1.4 Single-class PCA ........................................................... 66
    4.3.2 LDA ....................................................................... 68
4.4 Feature sets ................................................................. 69
5 Machine Learning Classification of Transient Survey Images

5.1 Introduction

5.2 Performance Measures

5.3 Training, Validation and Testing Procedures

5.4 Machine Learning Algorithms and their Implementations

5.4.1 Minimum Error Classification

5.4.1.1 The Algorithm

5.4.1.2 Testing

5.4.2 Naïve Bayes

5.4.2.1 The Algorithm

5.4.2.2 Testing

5.4.3 Support Vector Machine

5.4.3.1 The Algorithm

5.4.3.2 Testing

5.4.4 k-Nearest Neighbours

5.4.4.1 The Algorithm

5.4.4.2 Testing

5.4.5 Artificial Neural Network - SkyNet

5.4.5.1 The Algorithm

5.4.5.2 Testing

5.5 Results and Analysis

5.5.1 Best-Performing Classifier

5.5.2 Inter-Classifier Agreement

5.5.3 Classifier Performance on Different Visual Classes.

5.5.4 Incorrectly Classified Images

5.5.5 Comparison with Human Classifiers.

5.5.6 Performance on Spectroscopically Confirmed SNe

5.5.7 Classifier Run Time Considerations

6 Conclusions and Future Work

A Mathematical Background on Support Vector Machines

A.1 Derivation of Support Vector Machine Constraints for Linearly Separable Training Data

A.2 Determination of Support Vector Machine Parameters for Linearly Separable Training Data

A.3 Determination of Support Vector Machine Parameters for Linearly Non-Separable Training Data

A.4 Constructing New Kernels

A.5 Karush-Kuhn-Tucker Conditions

B Artificial Neural Network Training

B.1 Network Training

B.2 Error Backpropagation

C Hand-Scanner Classification
List of Figures

2.1 Handwritten digits. .............................................. 12
2.2 A $k$-nearest neighbours classification example. ............ 19
2.3 The concept of a margin. ...................................... 22
2.4 Maximised margins and support vectors. ....................... 23
2.5 The kernel trick. .................................................. 25
2.6 Slack variables. ................................................... 26
2.7 $N$-fold cross-validation. ...................................... 28
2.8 The perceptron. ................................................... 30
2.9 A 3-layer feed-forward neural network. ......................... 31
2.10 An autoencoder. .................................................. 34
2.11 LDA ................................................................. 40

3.1 The Crab Nebula and Crab Pulsar. .............................. 43
3.2 Schematic light-curves of SNe. .................................... 45
3.3 Standardisation of SNe lightcurves. ............................... 48
3.4 The SDSS photometric camera. .................................... 54
3.5 Simplified hand-scanning flow-chart. ............................. 57
3.6 Visual classification. .............................................. 58
3.7 Training, test and validation set. ................................. 59

4.1 Image cropping. ..................................................... 63
4.2 PC weights. .......................................................... 64
4.3 Principal Component Analysis .................................... 67
4.4 Obtaining different feature sets. ................................ 69

5.1 ROC curve for the various classifiers. ......................... 86
5.2 Cohen’s Kappa. ...................................................... 89
5.3 Real objects classified as not-real. ............................... 91
5.4 Not-real objects classified as real. ............................... 92

B.1 Backpropagation. .................................................... 114
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Characteristics of different types of SNe.</td>
<td>44</td>
</tr>
<tr>
<td>3.2</td>
<td>The different classification systems for objects in the dataset.</td>
<td>60</td>
</tr>
<tr>
<td>5.1</td>
<td>A confusion matrix.</td>
<td>72</td>
</tr>
<tr>
<td>5.2</td>
<td>The confusion matrix for MEC.</td>
<td>75</td>
</tr>
<tr>
<td>5.3</td>
<td>The confusion matrix for NB.</td>
<td>77</td>
</tr>
<tr>
<td>5.4</td>
<td>The confusion matrix for SVM.</td>
<td>79</td>
</tr>
<tr>
<td>5.5</td>
<td>The confusion matrix for kNN.</td>
<td>80</td>
</tr>
<tr>
<td>5.6</td>
<td>The confusion matrix for SkyNet.</td>
<td>83</td>
</tr>
<tr>
<td>5.7</td>
<td>Results table.</td>
<td>87</td>
</tr>
<tr>
<td>5.8</td>
<td>Example classification results.</td>
<td>87</td>
</tr>
<tr>
<td>5.9</td>
<td>Interpretation of the Cohen’s Kappa value.</td>
<td>88</td>
</tr>
<tr>
<td>5.10</td>
<td>Classifier performance on visual classes.</td>
<td>90</td>
</tr>
<tr>
<td>5.11</td>
<td>Performance comparison with humans.</td>
<td>92</td>
</tr>
<tr>
<td>5.12</td>
<td>Classifier performance on spectroscopically confirmed SNe.</td>
<td>93</td>
</tr>
<tr>
<td>5.13</td>
<td>Classifier run times.</td>
<td>93</td>
</tr>
<tr>
<td>C.1</td>
<td>SDSS hand-scanner classes for different SNR values.</td>
<td>116</td>
</tr>
<tr>
<td>C.2</td>
<td>SDSS hand-scanner classes in different bands.</td>
<td>117</td>
</tr>
</tbody>
</table>
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGN</td>
<td>Active Galactic Nuclei</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>ANN</td>
<td>Artificial Neural Network</td>
</tr>
<tr>
<td>AUC</td>
<td>Area Under Curve</td>
</tr>
<tr>
<td>DES</td>
<td>Dark Energy Survey</td>
</tr>
<tr>
<td>FLD</td>
<td>Fisher’s Linear Discriminant</td>
</tr>
<tr>
<td>FPR</td>
<td>False Positive Rate</td>
</tr>
<tr>
<td>KKT</td>
<td>Karush-Kuhn-Tucker</td>
</tr>
<tr>
<td>kNN</td>
<td>k-Nearest Neighbours</td>
</tr>
<tr>
<td>LDA</td>
<td>Linear Discriminant Analysis</td>
</tr>
<tr>
<td>LSST</td>
<td>Large Synoptic Survey Telescope</td>
</tr>
<tr>
<td>MEC</td>
<td>Minimum Error Classification</td>
</tr>
<tr>
<td>NB</td>
<td>Naive Bayes Classifier</td>
</tr>
<tr>
<td>PCA</td>
<td>Principal Component Analysis</td>
</tr>
<tr>
<td>Pan-STARRS</td>
<td>Panoramic Survey Telescope &amp; Rapid Response System</td>
</tr>
<tr>
<td>PTF</td>
<td>Palomar Transient Factory</td>
</tr>
<tr>
<td>ROC</td>
<td>Receiver Operator Characteristic</td>
</tr>
<tr>
<td>RNN</td>
<td>Recurrent Neural Network</td>
</tr>
<tr>
<td>SDSS</td>
<td>Sloan Digital Sky Survey</td>
</tr>
<tr>
<td>SLSN</td>
<td>Superluminous Supernova</td>
</tr>
<tr>
<td>SN</td>
<td>Supernova</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to Noise Ratio</td>
</tr>
<tr>
<td>SVM</td>
<td>Support Vector Machine</td>
</tr>
<tr>
<td>TPR</td>
<td>True Positive Rate</td>
</tr>
</tbody>
</table>
Physical Constants

Solar Mass \( M_\odot = (1.98855 \pm 0.00025) \times 10^{30} \text{ kg} \)

Hubble Constant \( H_0 = 67.80 \pm 0.77 \text{ km s}^{-1} \text{ Mpc}^{-1} \)

Parsec \( pc \approx 3.1 \times 10^{16} \text{ m} \)

Speed of Light \( c = 2.99792458 \times 10^8 \text{ m s}^{-1} \)
To my parents
Chapter 1

The History of Machine Learning

For seeing life is but a motion of limbs, the beginning whereof is in some principle part within, why may we not say that all automata (engines that move themselves by springs and wheels as doth a watch) have an artifical life? For what is the heart, but a spring; and the nerves, but so many strings; and the joints, but so many wheels, giving motion to the whole body...

– Thomas Hobbes, The Leviathan

1.1 Introduction

The field of machine learning concerns itself with the construction of computer programs that automatically improve their performance with experience. It draws on many ideas and concepts from many fields, including philosophy, biology, mathematics, statistics, control theory, computational complexity and logic, among others. It plays an increasingly important role in our modern society and finds applications in diverse areas such as computer vision, natural language processing, search engines, medical diagnosis, stock market analysis, pattern and speech recognition, robot locomotion and information retrieval.

It is impossible to have a clear idea of what machine learning is and where it comes from without looking at its slightly older and wiser uncle, Artificial Intelligence (AI), from which it grew. Although AI lacks a clear-cut and agreed-upon definition, it can broadly be seen as the field devoted to the study and design of intelligent agents, where intelligence can be taken as that attribute an entity requires in order for it to function properly and with foresight in its environment. According to this definition, intelligence lends itself to many things: human beings, animals, and certain machines. They all have varying degrees of intelligence, and cover different ranges of whom many are overlapping and have unclear boundaries. Because of a lack of sharp discontinuities between
Chapter 1. The History of Machine Learning

these ranges, it is better to have a broad view of what intelligence is and what AI, therefore, constitutes. [2]

This chapter will present a short history of AI and machine learning in order to orientate the reader, and to give some insight as to the origins and importance of these two intertwined, and often indistinguishable, fields. It will outline humanity’s AI dreams and achievements, look at the ideas and factors that influenced the field’s evolution over the years, and discuss machine learning and its place in the broader AI spectrum from which it branches. It should be noted that the primary source of information for this section was the book by Russell and Norvig [3], and that where not indicated otherwise, it should be assumed that information given was obtained from this source.

1.2 AI and Machine Learning: A Modern History

As mentioned above, AI and machine learning can in many cases be seen as two quite indistinguishable fields, sharing many methods and ideas - especially during their early years. We therefore detail the development of both these fields, as it is impossible to cover one field without involving the other. We will often use the terms “AI” and “machine learning” interchangeably, and will cover the period of development from 1943 up to the present. It should be noted, of course, that this history is by no means exhaustive, and that some facts, ideas and people of importance had to be omitted for the sake of brevity.

1.2.1 The Gestation Period (1943-1955)

The first work now generally recognised as modern AI and machine learning was done by Warren McCulloch and Walter Pitts in 1943 [4]. They put forth a network of artificial neurons, where each neuron is either “on” or “off”, a switch to “on” taking place when a neuron is stimulated by sufficiently many neighbouring neurons. They showed that any given function could be calculated by some neuron network and that all logical operators could be expressed with simple networks. More than that, they suggested that networks can be made to learn - and indeed, in 1949 Donald Hebb developed Hebbian Learning [5], showing that by using an updating rule to modify the strengths of the connections between neurons, learning was indeed possible. These discoveries put a start to the field of Artificial Neural Networks (ANNs), a family of statistical machine learning algorithms widely used today (ANNs are discussed in section 2.2.4). Soon after, in 1951, Marvin Minsky and Dean Edmonds developed the first ever neural network computer, called the SNARC (Stochastic Neural Analogue Reinforcement Computer). It consisted of 40 neurons, employed Hebbian Learning, and was able to learn some simple concepts [6, 7].
Amongst other early work considered to be AI, Alan Turing’s vision was of particular importance. In a paper he wrote in 1950 [8], he introduced the famous Turing Test\(^1\) and the concept of machine learning.

### 1.2.2 The Dawn of Artificial Intelligence (1956)

In 1956, John McCarthy, Marvin Minsky, Nathaniel Rochester and Claude Shannon organised a workshop at Dartmouth College for researchers interested in neural nets, automata theory\(^2\) and the study of intelligence - the workshop’s proposal [9] includes the first official use of the term artificial intelligence. The 10 attendees included Arthur Samuel (IBM\(^3\)), Trenchard More (Princeton) and Oliver Selfridge and Ray Solomonoff (MIT\(^4\)). Herbert Simon and Allen Newell, two attendees from Carnegie Tech\(^5\), already had a reasoning program named the Logic Theorist (LT) [10] which, soon after the workshop, was able to prove most theorems in Chapter 2 of Principia Mathematica [11] - LT even found a shorter proof for one of the theorems.

The Dartmouth workshop itself did not lead to any breakthroughs, but it introduced all the major figures in the field to one another. The attendees, their colleagues and their students at MIT, IBM, CMU and Stanford University would dominate the field for the coming 20 years. The workshop also established AI as a separate field, with goals distinct from fields like control theory, operations research, decision theory and mathematics in that it strives to address issues like the duplication of human faculties (e.g. self-improvement, creativity, and language use) and in the process attempts to create machines that function autonomously.

### 1.2.3 Early Days and Expectations (1952-1969)

Simon and Newell followed up their earlier successes by developing the General Problem Solver (GPS) [12] which, unlike LT, was programmed from the start to emulate protocols of human problem-solving. GPS and the cognition model programs that followed led to their formulation of the physical symbol system hypothesis [13, 14], stating that a system, whether it be human or machine, displaying intelligence must function through the manipulation of data structures consisting of symbols.

---

\(^1\)Highly influential and widely criticised, the Turing test examines a machine’s ability to display intelligent behaviour indistinguishable from a human’s. In the original setting, a human judge has conversations with a machine and a human, with all participants separated from each other. If the judge can’t distinguish between the human and the machine, the machine has passed the Turing test. The Russian chatter bot Eugene Goostman, developed by Vladimir Veselov et al., came closest yet to passing the Turing test in 2014 by fooling 33 % of the judges at the “Turing 2014: Can Machines Think?” event (visit [http://www.robolaw.eu/news.htm#turing2014](http://www.robolaw.eu/news.htm#turing2014)).

\(^2\)The study of self-operating machines and the computational problems they can solve.

\(^3\)International Business Machines Corporation.

\(^4\)Massachusetts Institute of Technology.

\(^5\)Now Carnegie Mellon University (CMU).
At IBM development also went forwards, with some of the earliest AI programs having been created by Nathaniel Rochester and his colleagues. Herbert Gelernter developed the Geometry Theorem Solver in 1959 [15], a program that was capable of proving theorems that many students of mathematics would find challenging, and in 1952 Arthur Samuel (using decision-theoretic techniques) wrote checkers programs [16, 17] that quickly learned how to play a better game than he could himself, disproving the idea that computers could only do what they were told to. Samuel’s efforts were among the first in what would later become the field of machine learning. In 1958 John McCarthy, now at MIT, developed the Lisp programming language and invented, together with others at MIT, time sharing. In the same year he also described a hypothetical program called the Advice Taker [18], seen by some as the first complete AI system. It used knowledge to find solutions to problems, but unlike LT and the Geometry Theorem Solver it made use of general world knowledge - it was designed to accept new axioms during the course of its operations, allowing it to become competent in new areas. The program therefore made use of the key principles of reasoning and knowledge representation: a formal representation of the world together with the ability to manipulate it.

In the 1960’s Minsky, now also at MIT, supervised students who studied problems that seemed to require intelligence in order to be solved. These problems were called microworlds, the most famous one having been the “blocks world”, comprising of a set of blocks on a table-top operated by a robot hand. It was home to David Huffman’s vision project [19] and Terry Winograd’s natural-language-understanding program, SHRDLU [20], among others.

Meanwhile, work that built on McCulloch and Pitts’s neural networks also flourished - Winograd and Cowan [21] showed that an individual concept could be represented by a large number of collective elements and Hebb’s learning methods were improved by Bernie Widrow [22, 23] and by Frank Rosenblatt [24], who introduced perceptrons. The perceptron convergence theorem [25], published by Block et al. in 1962, states that a learning method can modify a perceptron’s connection strengths to match any input data, if such a match exists.

1.2.4 Reality Strikes (1966-1973)

The promising performance of early AI solutions to elementary problems led to a general overconfidence in the community of what was achievable at the time. In most cases these early AI systems failed when applied to more diverse or more complex problems. This was due to a few difficulties.
The first was that, because most early language-processing AI programs didn’t know anything about their subject matter, they worked by using simple syntactic manipulations. An example is early machine translation efforts, where it was initially thought that word replacements and basic syntactical transformations based on the different languages’ grammar would be sufficient to preserve exact sentence meanings. The truth is that background knowledge is required for accurate translation, so that language phenomena like ambiguity doesn’t stand in the way of determining a sentence’s content. Although it has found widespread use, machine translation remains imperfect until this day.

The second difficulty arose from the intractable nature of most problems AI was trying to solve. Many early AI algorithms solved problems by attempting steps in different combinations until they arrived at the solution - this worked due to the fact that many problems was of a simple nature requiring short solution sequences. Before the advent of the field of computational complexity, it was assumed that larger problems would simply require larger memories and faster hardware. It was soon realised to be a misconception, an example being the dampened optimism accompanying the development of resolution theorem proving when programs couldn’t prove theorems containing more than a dozen or so facts. This assumption was not limited to problem-solving programs - early development in genetic algorithms [26, 27] were grounded on the correct idea that by making a series of mutations to a program, one could evolve it to have a good performance on any specific task. This was carried out by trying random mutations and keeping the useful ones. During early development almost no progress was made, despite thousands of CPU hours - modern genetic algorithms, however, have shown more success by using better representations and plays an important role in modern approaches to machine learning.

Lastly, problems arose because of the fact that basic AI structures that was being used for the generation of intelligence had some fundamental limitations. An example of this is the book “Perceptrons” by Minsky and Papert in 1969 [28], in which they proved that although perceptrons have the ability to learn anything they could represent, they could represent very little, causing research funding for neural networks to become almost non-existent. The backpropagation algorithms\(^8\) for multilayer networks that resulted in a resurgence of neural network research in the 1980s was, ironically, discovered in 1969 by Bryson and Ho [29].

1.2.5 Knowledge-Based Systems (1969-1979) and the AI Industry (1980-present)

The first decade of AI research was dominated by approaches using general-purpose search methods stringing together simple reasoning steps in order to arrive at complete solutions. These algorithms have been called weak methods due to their inability to scale up to larger or more complicated problems. Alternatively, methods using powerful, domain-specific knowledge can be used - this\(^8\) An abbreviation of “backward propagation of errors”, this is a common method used for the training of ANNs. See section B.2 for more details.
allows larger reasoning steps to be taken and results in better performance on typically occurring problems in narrower areas of expertise.

The DENDRAL program, developed by Buchanan et al. in 1969 [30], is an example of such an expert system. DENDRAL was used to help tackle the problem of inferring molecular structure using spectrometer information. Its significance lies in the fact that it was the first successful knowledge-intensive program - it made use of many special-purpose rules to perform well on the problem.

Shortly after, Feigenbaum and his colleagues at Stanford started the Heuristic Programming Project (HPP) in order to determine to what extent expert systems could be used for other domains of human expertise. In the area of medical diagnosis, Feigenbaum, Shortliffe and Buchanan created the MYCIN [31, 32], a program running on 450 rules that could diagnose blood infections with a performance equivalent to that of some human experts in the field. Expert systems also made an appearance in the field of natural language processing. Terry Winograd’s program SHRDLU (mentioned earlier as part of the blocks microworld) overcame ambiguity and understood pronoun preferences, although this was mainly the result of it being developed for one very specific area - the blocks world. Its dependence on syntactical analysis caused some of the same problems as mentioned before. Others suggested that a robust understanding of language would require general world knowledge, and corresponding methods for the usage of such knowledge. One of these researchers was Robert Schank who, with his students, built programs [33–36] all with the task of understanding natural language - with the emphasis more on representing and reasoning with the knowledge necessary for comprehending natural language than on language itself.

Due to the commercialisation of expert systems, the AI industry grew from a worth of millions of dollars in 1980 to a worth of billions in 1988. Soon after, though, companies became unprofitable as they couldn’t deliver on their extravagant promises. People lost faith in AI and the following years saw a corresponding drop in funding for AI research and projects - a time now referred to as the “AI winter”. This draught was, in part, also due to the nature of AI - being founded, in part, as a field in rebellion against the limitations of existing fields like statistics and control theory, it has not yet reached a point of integration with these helpful approaches.

1.2.6 The Rise of Machine Learning (1980-present)

Up to this point I have (mostly) used the term “AI” as an overarching name for AI and all of its constituents - seeing as AI was still a forming field and boundaries between it and other fields not clear at all times, this was acceptable. We have now, however, reached a point in history where the distinguishing line between machine learning and its parent field AI becomes more apparent.
In 1980, the first machine learning workshop held at CMU identified a group of researchers with a shared interest in computational approaches to learning - at the time, the parent field of AI was showing little interest in learning-related issues, choosing instead to concentrate on logical, knowledge-based approaches such as those required for the design of expert systems. The use of statistics in AI fell out of favour, and though work on the symbolic/knowledge-based approach to learning did continue, its statistical line of research was now outside the domain of AI, in pattern recognition and information retrieval. Machine learning changed its former goal of achieving artificial intelligence to that of solving problems of a more practical nature. It shifted its focus away from the symbolic approaches it inherited from AI, and drifted towards methods borrowed from statistics, pattern recognition and probability theory. \[37\] It should be noted that recent advances in AI, however, have seen it re-establishing common ground with other disciplines such that the field is now commonly referred to as “Modern AI” - machine learning and AI are once again very integrated.

During the mid-1980s, the backpropagation algorithm originally discovered by Bryson and Ho in 1969 \[29\] was reinvented by four different research groups. It was used for many problems in computer science, and the collection of the results, entitled “Parallel Distributed Processing”, by Rumelhart and McClelland in 1986 \[38\] caused great enthusiasm and set the stage for neural network research to flourish once more - today ANNs are valuable machine learning techniques.

Machine learning, by now a well-defined research field, began to flourish in the 1990s. Whereas before 1980 it was mainly represented by neural network methods, it quickly broadened its arsenal to include (to name but a few) memory-based learning (e.g. the \(k\)-nearest neighbours method - section 2.2.2), case-based reasoning\(^9\), decision tree learning\(^{10}\), support vector machines (section 2.2.3), unsupervised and reinforcement learning methods (section 2.1.2) and deep learning techniques\(^{11}\) \[2\]. The success of machine learning has also been helped along by the advent of large data sets in the mid 1990’s to early 2000s. The more data available for training, the more likely it becomes that learning algorithms will be able to learn successfully from it. This also led to the relaxed optimisation of the learning rate of algorithms - where before algorithms had to use small datasets and therefore had to have high learning rates to be successful, they now have the luxury of vast datasets that relaxes the emphasis on efficient learning. The more data, the better - an aspect that made machine learning techniques ideal for data mining\(^{12}\) applications \[37\].

\(^9\)Broadly speaking, the process by which the solutions to past problems are used to find solutions to similar new ones.

\(^{10}\)Learning that uses a decision tree as a predictive model to map observations representing a data instance to conclusions about the item’s nature.

\(^{11}\)Algorithms modelling high-level data abstractions using models consisting of numerous nonlinear functions.

\(^{12}\)The computational process by which patterns in large data sets are discovered, usually using methods from AI, statistics and machine learning.
Today, machine learning applications are widely used all around us. Learning techniques classify over a billion messages as junk e-mail every day [39, 40] and self-driving vehicles are making headlines: a robotic vehicle named Stanley (developed by Stanford researchers) succeeded in winning the 2005 DARPA Grand Challenge\footnote{\url{http://www.darpa.mil/About/History/Archives.aspx}} [41], the autonomous vehicle called Boss (developed by CMU) won the DARPA Urban Challenge\footnote{\url{http://archive.darpa.mil/grandchallenge/}} the next year [42] and the “Google Self-Driving Car” project continues to improve on the design of cars that can function autonomously in city environments\footnote{Google: \url{http://www.google.com/about/company/} Google research: \url{http://research.google.com/}}.

In game-playing, IBM’s chess program named “Deep Blue” became the first computer program to beat a world champion (Garry Kasparov) in 1997 [43], and applications of machine learning algorithms in the areas of language translation, speech recognition, medical diagnosis, robot locomotion, data analysis, stock market analysis and software engineering abound. This is of course not an exhaustive list - machine learning is practically everywhere around us, and the coming years will see the continued growth of the field.

### 1.3 Machine Learning Applications in Astronomy

Applications of machine learning in astronomy is of particular interest to this thesis, and so this section discusses the usage of these algorithms in different areas and for different problems in the field as a whole. This is by no means a complete overview of such work, and serves merely to give the reader an idea of the applicability of machine learning algorithms in the field. This section mentions various machine learning algorithms - the reader should note that neural networks (section 2.2.4), principal component analysis (section 2.3.1), k-nearest neighbours (section 2.2.2) and support vector machines (section 2.2.3) will be covered later in the thesis, as indicated. The work of Ball & Brunner [44] was used as a source of information for this section.

#### 1.3.1 Classification of Objects

A well-studied application of machine learning in astronomy is that of star-galaxy separation - the large number of stars (appearing as point sources) and galaxies (appearing as extended sources) in photometric catalogues make this a problem requiring automation. Several algorithms, including neural networks [45–51] and decision trees [52, 53], have been used to tackle this problem, with most of these algorithms achieving a precision score of more than 95\%\footnote{The fraction of relevant retrieved instances. See section 5.2 for a full description of the precision performance metric.}, typically done using algorithm inputs of morphological parameters derived from the survey photometry.

A second problem that machine learning is often applied to is that of distinguishing between different galaxy morphologies. Galaxies come in many shapes and sizes, and knowledge of a particular...
Chapter 1. The History of Machine Learning

galaxy’s morphology can give information as to its formation and evolution. Using machine learning algorithms, one can assign galaxy morphologies to images when measured parameters (such as morphological parameters or colour information) are available - using neural networks on low redshift\textsuperscript{17} data, Lahav and his collaborators wrote a series of papers [54–59] carrying out the above, and found that it is possible to obtain a classification accuracy similar to that of human experts. Other studies have applied neural networks to higher redshift data [60], and morphological types have also been assigned to galaxies by neural networks using galaxy spectra as input [61]. Galaxy morphology at higher redshift is also studied by using data from the Hubble Deep Field\textsuperscript{18} where galaxies are fainter, more distant, morphologically more peculiar and less evolved - three papers [62–64] use surface brightness and light profiles of galaxies as inputs to neural networks in order to classify them. Other classifications of galaxies have also been tackled with machine learning - numerous papers [65–68] applied principal component analysis directly in order to obtain the spectral classifications of galaxies.

Most of the electromagnetic radiation in the Universe is emitted by either stars or by the accretion disks around supermassive black holes in Active Galactic Nuclei\textsuperscript{19} (AGN). In the case of quasars\textsuperscript{20} for the latter, the central region of the galaxy can outshine the entire galaxy it resides in. Due to the fact that supermassive black holes are thought to be pervasive in larger galaxies, and because their intrinsic brightness can be influenced by the host galaxy’s environment, AGN and quasars are important tools for understanding the evolution and formation of structure in the Universe. The identification of AGN and quasars in astronomical surveys is therefore an important and well-studied problem. Several people have used neural networks [69–71] and decision trees [72–74] for the selection of quasars from surveys, where many of the above studies combine multi-wavelength data. In a similar fashion, the selection and classification of AGN can be done - a paper by Zhao et al. [75] details the spectral classification of AGN using a k-nearest neighbours method.

1.3.2 Photometric Redshifts

Redshift estimation using photometric data is an area of study that has become more and more popular during the last few years. This reason for this is that, even though photometric redshifts are less accurate than the ones obtained with the use of spectra, the vast number of objects for which photometric measurements are available make up for the loss in individual accuracy through statistical noise suppression in ensemble calculations.

\textsuperscript{17}See Eq. 3.10 for the definition of redshift.
\textsuperscript{18}An image of a small region in the Ursa Major constellation, constructed from 342 exposures taken by the Hubble Space Telescope.
\textsuperscript{19}These are galaxies with very bright and energetic central regions, caused by either the presence of a black hole or by star formation at their cores.
\textsuperscript{20}Quasars (quasi-stellar radio sources) are the most distant and energetic AGNs found. The are extremely luminous, and emit electromagnetic energy giving them an appearance more star-like than galaxy-like - from there the term “quasi-stellar”.
For normal galaxies at low redshift, the calculation of photometric redshifts is simple due to the typical galaxy spectrum break at 4000 Å- resulting in a relatively smooth colour change as a galaxy is redshifted with increasing distance. Studies using neural networks [76–80], support vector machines [81, 82], decision trees [83] and k-nearest neighbours [84] have been used for the determination of photometric redshifts for such galaxies.

The determination of photometric redshifts for AGN or quasars is more complicated, seeing as their spectra are dominated by bright and narrow emission lines which dominate the colour in broad photometric passbands. Machine learning applications to tackle the problem of photometric redshift determination for these objects include the use of k-nearest neighbours, neural networks and decision trees [85].

1.3.3 Other Applications

There are many other applications of machine learning in astronomy. Examples include that of Ramirez, Fuentes & Gulati [86], where physical parameters of stellar atmospheres are predicted using spectral indices. Here, a genetic algorithm is used for the selection of appropriate input features, after which the parameters are predicted using a k-nearest neighbours algorithm. More examples are the work of Mokiem et al. [87], where a fitting method based on a genetic algorithm is used to spectrally analyse early-type stars, and the work of Giridhar et al. [90], where metal-poor stars are identified with the help of a neural network. Other interesting examples include SkyNet, a generic neural network training algorithm developed by Graff et al. [88] and Source Extractor (SExtractor) [89], used for object detection.

Machine learning applied to time domain data is also an area in which a lot of work has been done. In this area, machine learning has been applied to quasar variability, gamma ray bursts, supernovae, novae, extrasolar planets, stellar proper motions, solar system planetary atmospheres, detection and classification of asteroids, transient lunar phenomena, and the interaction of the solar wind and the Earth’s atmosphere. An overview of this can be found here [91].
Chapter 2

An Introduction to Machine Learning

2.1 Introduction

Machine learning is concerned with creating computer algorithms that can automatically discover regularities in data and, using these regularities, improve their performance on a given task by learning through experience. This section will introduce some common terms and concepts that will be encountered throughout this thesis, after which it will proceed to discuss the three broad categories of machine learning applications. The two following sections in this chapter will discuss the various machine learning algorithms used later in the thesis (section 2.2) and the feature extraction techniques employed (section 2.3). It should be noted that, where not mentioned otherwise, the main sources of information for this chapter were the books by Bishop [92] and Mitchell [93].

2.1.1 Important Concepts

As an example of a typical machine learning problem, consider the handwritten digits shown in Fig. 2.1. Each digit (referred to more generally as a data *instance*) comprises of a $28 \times 28$ pixel image,
and can therefore be represented with a 784-element vector $\mathbf{x}$. These elements, characterising the data instance, are normally referred to as its features. The objective here is to design an algorithm that takes such a feature vector $\mathbf{x}$ as an input and produces as the output a classification as one of ten possible classes, with each class corresponding to one of the digits $0, \ldots, 9$. This problem is difficult because of the large variability found in people’s handwriting. An attempt at a solution could be made by designing sets of rules or using heuristics in order to distinguish digits from one another - however, such methods often lead to an infeasible amount of rules and exceptions to those rules (and so on) resulting in complicated systems with poor performance.

![Figure 2.1: Handwritten digits.](image)

An example of handwritten digits from zip codes in the US, taken from [92].

Much better solutions to this problem is obtained by approaching it from a machine learning perspective, where a set of $T$ digits $\{\mathbf{x}_1, \ldots, \mathbf{x}_T\}$, referred to as the training set, is used for adjusting an adaptive model’s parameters. The corresponding category of each digit in the training set, referred to as the target value $t$ for each digit $\mathbf{x}$, is known beforehand and form part of the input to the algorithm.

The execution of the algorithm can then be represented by the function $y(\mathbf{x})$, where the digit $\mathbf{x}$ is fed as an input and the algorithm outputs a value $y$ (the identity of the digit) encoded in a way similar to that of the target values. The function’s form is determined in the training phase (also called the learning phase) using the training data, whereafter it can be used to determine the categories of a set of new digits, called a test set. The ability of an algorithm to correctly classify new instances different from those in the training set is referred to as generalisation, one of the central goals in machine learning. An important concept to note here is that of overfitting. Overfitting can occur when an algorithm is subjected to the learning phase for a too-extensive period of time or when the training set is too small. In cases like this, a learning algorithm often adjusts to certain arbitrary features in the data having no real relation to the problem’s target function. During overfitting, an algorithm’s performance on the training set will increase while its performance on the test set will decrease.
Usually, the original input features are *pre-processed* in order to express data instances in a new variable space where it would be simpler for the machine learning algorithm to solve the problem. As an example, the images in the above problem have been scaled and translated in order for all digits to be of the same, fixed size - the variability in each category of digits is therefore reduced, making it easier for the algorithm to distinguish correctly between different classes. This process is also sometimes referred to as *feature extraction*, and must be applied to the test set in the same way as it is applied to the training set.

Feature extraction is also carried out for the purpose of speeding up computational processes. In the case of real-time facial recognition, for example, a large number of pixels must be processed by the computer every second. Instead of feeding all these pixels directly into a complex machine learning algorithm, which might be computationally infeasible, one can extract features that can be calculated swiftly and that still preserves the necessary discriminatory information that would be useful for the algorithm when trying to distinguish between faces. These extracted features, of a number less than the original number of pixels in an image, are then the algorithm’s new inputs. This type of feature extraction is an example of dimensionality reduction - each face (or data *instance*) is now represented by a few features instead of all its pixels. One must take care to not discard valuable information during the feature extraction phase, as this will lead to an overall decrease in performance of the specific algorithm.

Another motivation for characterising instances with smaller rather than larger numbers of features is the range of phenomena referred to as the *curse of dimensionality*, a term coined by Richard Bellman in 1961 [94]. In the field of machine learning, as explained in the book by Hastie et al. [95], the curse refers to the complexity of learning functions that can grow exponentially with the input feature space dimension, such that in order to estimate these higher-dimensional functions with an accuracy similar to that of the functions in lower dimensions, the training set has to grow exponentially in size as well. Another way of seeing this is to note that some learning algorithms learning from a finite number of training instances with a higher-dimensional feature space (where every feature can take on one of many possible values) requires a vast amount of training data in order to ensure that several instances exist for every combination of possible feature values. If the size of the training set is fixed, the performance of an algorithm decreases as the dimensionality of the feature space increases. This is referred to as the Hughes effect [96]. Other examples of the curse of dimensionality also exist - see section 2.2.2 for a case of the curse that nearest neighbours learning algorithms are usually concerned with.

### 2.1.2 Learning Categories

Machine learning applications can be grouped into three broad learning categories. Firstly, problems where the training set consists of the input feature vectors $\mathbf{x}$ of the data instances along with
their respective target values \( t \) (that need to be predicted) are referred to as \textit{supervised learning}. Supervised learning problems like the digit example used above, where the goal is to map each input \( x \) to one of a number of discrete values (or categories) are known as \textit{classification}, whereas supervised problems in which the input vector is mapped to a real-valued output are known as \textit{regression} problems. An example of a regression problem would be the prediction of property prices in a given city where the size of the property and the distance from the centre of town is given as inputs to the algorithm. Seeing as this thesis is concerned with the problem of classification (as will be explained in Chapter 3), it is again briefly addressed in section 2.1.2.1.

Secondly, applications where the training set consists of the feature vectors \( x \) without their respective target values are referred to as \textit{unsupervised learning} problems. In this category, algorithms can fall into a further one of three broad groups. \textit{Clustering} refers to the finding of similar groups of data instances, for example the finding of tightly-knit communities within vast numbers of people using online social networks. \textit{Density estimation} is the process by which the distribution of the data in the input space is determined, a simple example being the use of a histogram to estimate a continuous variable’s probability distribution. \textit{Visualisation} refers to the projection of data from a higher-dimensional to a two- or three-dimensional space.

Lastly, \textit{reinforcement learning} [97] refers to problems trying to find suitable actions in given situations with the goal of maximising a reward over a certain period of time - here, the algorithm does not take optimal output examples during training, but instead has to discover them through trial and error. Reinforcement learning is applied to problems such as robot control, self-driving cars and games such as backgammon, chess and checkers, to name but a few.

### 2.1.2.1 Supervised Learning: Classification

As already mentioned above, classification problems have as their goal the assignment of a data instance \( x \) to one of \( M \) discrete classes \( C_m \), with \( m = 1, \ldots, M \). In most classification problems, classes are mutually exclusive, making it impossible to assign an input instance to more than one class. In these cases, we say that the input space is divided into areas called \textit{decision regions}, the boundaries of which are referred to as \textit{decision surfaces}. If the classes in a data set can be perfectly split apart from one another by using only linear decision surfaces, the data is \textit{linearly separable}. Classification problems can be further separated into two categories - in \textit{binary classification} an instance is assigned to one of only two possible classes, while \textit{multiclass classification} involves the mapping of an instance to one of several possible classes.

For this project, we are concerned with the problem of binary classification, as will be explained in Chapter 3. Many existing learning algorithms addresses this task. In the next section we discuss the naïve Bayes classifier, the \( k \)-nearest neighbours algorithm, the support vector machine and Artificial Neural Networks, as these were the algorithms selected for the purpose of this project.
Chapter 2. An Introduction to Machine Learning

2.2 Machine Learning Algorithms

This section discusses the naïve Bayes classifier (section 2.2.1), the $k$-nearest neighbours algorithm (section 2.2.2), support vector machines (section 2.2.3) and Artificial Neural Networks (section 2.2.4) for the purpose of machine learning classification. It should be noted that the sections describing these algorithms supply the standard theoretical background in order to provide a basis for understanding later chapters more easily. Discussions and explanations of the methods are kept general, with the specific implementation of each of the algorithms and their deviations from the standard theoretical models discussed in Chapter 5.

2.2.1 Naïve Bayes

Bayesian reasoning is built on the supposition that quantities of interest are controlled by probability distributions, and that taking observed data into consideration while working with these probabilities can result in optimal decisions being made. Its importance to machine learning is based on the fact that it can be used for providing quantitative approaches to weighing the evidence for different hypothesis. It provides the framework for algorithms directly calculating and manipulating probabilities.

This section will discuss the naïve Bayes classifier, a highly practical Bayesian classifier, starting first with an introduction to Bayes theorem.

2.2.1.1 Bayes Theorem: A Machine Learning Perspective

In machine learning we often want to determine the most suited, or the most probable, hypothesis (outcome) $h$ from some hypothesis space $H = \{h_1, h_2, \ldots, h_M\}$, given observed training data $D$ as well as any knowledge concerning the prior probabilities of the different hypotheses.

Bayes theorem gives us a way of calculating how probable different hypotheses are. By using the prior probability of a hypothesis, the observed training data and probabilities of observing certain data given the hypothesis, we can determine the hypothesis’s probability.

In order to express Bayes theorem mathematically, some notation should be introduced. $P(h)$ denotes the prior probability of hypothesis $h$ – that is, it is the probability of hypothesis $h$ being the correct one, before any training data have been observed. In the same way, $P(D)$ denotes the prior probability of observing the training data, given no information as to which hypothesis is the correct one, while $P(D|h)$ is the probability that $D$, the training data, will be observed given that hypothesis $h$ holds. Our main interest here, however, is in finding the posterior probability of a certain hypothesis $h$, denoted by $P(h|D)$, as this is a reflection of our confidence that a specific
hypothesis holds after seeing the training data $D$. Bayes theorem gives us a method of calculating $P(h|D)$ using the prior probabilities $P(h)$ and $P(D)$, as well as $P(D|h)$, and is defined in Eq. 2.1.

$$P(h|D) = \frac{P(D|h)P(h)}{P(D)} \quad (2.1)$$

In many classification machine learning problems, the learning algorithm considers a set of hypotheses (classes) $H$ and tries to find the hypothesis $h \in H$ that is most probable to be correct, given the training data $D$. Such a most probable hypothesis can be referred to as a “maximum a posteriori” (MAP) hypothesis, and can be determined by calculating each hypothesis’s posterior probability with the use of Bayes theorem. Mathematically, $h_{MAP}$ is a MAP hypothesis if

$$h_{MAP} = \arg\max_{h \in H} P(h|D)$$

$$= \arg\max_{h \in H} \frac{P(D|h)P(h)}{P(D)} \quad (2.2)$$

Here, argmax is short for the “argument of the maximum”, an operator returning the points of the argument that maximises the given function. For example,

$$\arg\max_x f(x) \quad (2.3)$$

are those points $x$ that will maximise the function $f(x)$. The operator argmin (“argument of the minimum”) can be defined analogously. Noting next that the term $P(D)$ in Eq. 2.2 is constant and not dependent on $h$, we can drop it and simplify the equation to

$$h_{MAP} = \arg\max_{h \in H} P(D|h)P(h). \quad (2.4)$$

Sometimes, for example when we have no prior information about any of the candidate hypotheses in $H$, it is appropriate to assume that all of them have an equal a priori probability of being correct. That is, $P(h_j) = P(h_i)$ for all $h_j$ and $h_i$ in $H$. In such cases Eq. 2.4 can be further simplified by dropping the term $P(h)$ so that only $P(D|h)$ needs to be considered for finding the MAP hypothesis. $P(D|h)$ is also referred to as the likelihood of $D$ given $h$, and the hypothesis maximising $P(D|h)$ is known as the maximum likelihood (ML) hypothesis, $h_{ML}$. Taking all this into account, Eq. 2.4 can now be re-written as follows:

$$h_{ML} = \arg\max_{h \in H} P(D|h) \quad (2.5)$$
2.2.1.2 The Naïve Bayes Classifier

The naïve Bayes classifier is a Bayesian learning algorithm that can be applied to learning problems where each data instance is characterised by a feature vector $x$, and where $y(x)$, the target function, can be assigned any one of $M$ discrete target values $C_m$, where $m = 1, \ldots, M$ (this can be seen as equivalent to the hypothesis space $H$ mentioned in section 2.2.1.1).

Training instances for each of the possible target values of the target function is provided to train the classifier, after which a new instance, described by a feature vector $x = (x_1, x_2, \ldots, x_N)$, is presented. The classifier is then asked to classify the new instance.

Using the Bayesian approach, this classification is done by finding the target value with the highest probability of being correct, $C_{MAP}$, given the feature values $(x_1, x_2, \ldots, x_N)$ describing the instance. This is expressed mathematically as follows:

$$C_{MAP} = \arg\max_{C_m} P(C_m|x_1, x_2, \ldots, x_N)$$

Using Bayes theorem, defined in Eq. 2.1, and applying the same simplification that was used to get to Eq. 2.4, we can rewrite Eq. 2.6 as

$$C_{MAP} = \arg\max_{C_m} \frac{P(x_1, x_2, \ldots, x_N|C_m)P(C_m)}{P(x_1, x_2, \ldots, x_N)}$$

$$= \arg\max_{C_m} P(x_1, x_2, \ldots, x_N|C_m)P(C_m)$$

The two terms in the last line of Eq. 2.7 can now be estimated with the help of the training data. The $P(C_m)$ terms can easily be estimated merely by determining the frequency of occurrence of each target value $C_m$ in the training data. It is, however, not feasible to determine the large number of $P(x_1, x_2, \ldots, x_N|C_m)$ terms\(^1\) in this way if we do not have a very large training data set, as reliable estimates can only be made if every possible instance in the instance space is observed many times in the training set.

If we now assume conditional independence of the feature values given $C_m$, the probability of observing the feature vector $(x_1, x_2, \ldots, x_N)$ given the target value of the instance is merely the product of the individual features’ probabilities, as follows:

$$P(x_1, x_2, \ldots, x_N|C_m) = \prod_i P(x_i|C_m)$$

\(^1\)The number of possible classes multiplied by the number of possible data instances.
We can substitute Eq. 2.8 into Eq. 2.7 to obtain the naïve Bayes classifier’s approach to classification, shown in Eq. 2.9.

\[
C_{NB} = \arg\max_{C_m} P(C_m) \prod_i P(x_i|C_m)
\] (2.9)

Here, \(C_{NB}\) is the class output of the learning algorithm. Now, instead of having to calculate a large number of \(P(x_1, x_2, \ldots, x_N|C_m)\) terms as before, we have to estimate the \(P(x_i|C_m)\) terms. Seeing as the number of these terms is merely the number of classes multiplied by the number of feature values, we are now left to estimate a much smaller number of terms than before.

In summary, the training phase of the naïve Bayes classifier consists of estimating the \(P(C_m)\) and \(P(x_i|C_m)\) terms - this is done by counting their respective frequencies in the training data. The exact way in which this is done varies in practice - to see how we implemented the estimation of these terms, see section 5.4.2.1. Once the learning algorithm is trained, it can be used for the classification of new data instances by using the approach in Eq. 2.9, where \(C_{NB}\) is the same as the MAP classification if the simplifying assumption of conditional independence discussed earlier is satisfied.

This simplifying assumption is also the one major setback of the naïve Bayes classifier. Feature values (given a class \(C_m\)) are rarely conditionally independent in real-life problems, an issue that often leads to the reduced performance of the classifier.

### 2.2.2 k-Nearest Neighbours

The \(k\)-nearest neighbours algorithm is an extremely simple machine learning algorithm. A new unclassified test instance \(x\) is classified by carrying out a majority class vote among the \(k\) training instances that are closest to it in feature space. These \(k\) training instances are referred to as its \(k\) nearest neighbours. [95]

To intuitively illustrate the working of the algorithm, see Fig. 2.2, a visualisation of the classification of a test instance \(x_0\) by a 5-nearest neighbours \((k = 5)\) algorithm. Here, the training instances are two-dimensional data points (each instance is represented by \(N = 2\) features) with either a positive or a negative class-value, denoted by “+” and “-”, respectively. In this case \(x_0\) will be classified as “+”, as three of its five nearest neighbours (encircled in the figure) is of the “+” class while only two of its nearest neighbours are of the “-” class - a majority class vote is therefore in favour of the positive class.
Figure 2.2: A k-nearest neighbours classification example.

An example classification of a test instance $x_0$ by a 5-nearest neighbours ($k = 5$) algorithm into either a positive or a negative class, denoted by “+” and “−” respectively. Because the majority of the five closest training instances (encircled) are positive, $x_0$ will be classified as belonging to the positive class.

In order to determine the $k$ nearest neighbours of a particular test instance, one has to select the $k$ training instances that are closest in distance to it in feature space (as mentioned above). If the test instance $x$ has a feature vector

$$ (x_1, x_2, ..., x_N) $$(2.10)

where $x_n$ is the $n$’th feature of $x$, then the Euclidean distance between $x$ and a training instance $x_j$ is denoted as $d(x, x_j)$, given as

$$ d(x, x_j) = \sqrt{\sum_{n=1}^{N} (x_n - x_{j,n})^2}. $$ (2.11)

To mathematically express the intuitive picture in Fig. 2.2, we consider only discrete-valued target functions (for classification, as mentioned before) denoted by $y(x)$, where $y$ can be assigned any one of $M$ discrete target values $C_m$, where $m = 1, \ldots, M$. The $k$-nearest neighbours algorithm for the target function of a new test instance $x$ can then be expressed as

$$ y(x) = \arg \max_{C_m} \sum_{r=1}^{k} \delta(C_m, t_r) $$ (2.12)

where $t_r$ is the class value (target value) of the $r$’th nearest neighbour and $\delta(a, b) = 1$ if $a = b$ and $\delta(a, b) = 0$ otherwise. It can therefore be seen that $y(x)$ is simply the most common class value of $x$’s $k$-nearest neighbours.
Chapter 2. *An Introduction to Machine Learning*

Considering Fig. 2.2 one last time, it can be seen that in the case of using a 2-nearest neighbours algorithm \((k = 2)\), there would be an equal count of “+” and “-” classes among the neighbours of \(x_0\). There are different ways of solving this problem. One can, for example, increase or decrease \(k\) so that a majority vote will be able to yield one class as the winner. A good way of mostly avoiding such a problem, however, is to make use of a common extension to the \(k\)-nearest neighbours algorithm: weighting the contribution of each of the \(k\)-nearest neighbours with regard to their distance from the test instance. Introducing such weights, Eq. 2.12 then becomes

\[
y(x) = \arg\max_{C_m} \sum_{r=1}^{k} w_r \delta(C_m, t_r),
\]

where \(w_r\) is the weight of the \(r\)’th nearest neighbour. One possible example of such a weight can be seen in Eq. 2.14, where the importance of nearest neighbours will be scaled by the inverse square of the distance between the particular neighbour \(x_r\) and the test instance \(x\).

\[
w_r = \frac{1}{d(x, x_r)^2}.
\]

2.2.2.1 Remarks on the Algorithm

One possible disadvantage of the \(k\)-nearest neighbours method is concerned with the fact that all the features of instances are used when calculating the Euclidean distance between data points. If it so happens that only a small set of the features contain discriminatory information while the remaining majority of features are irrelevant, the distance between instances end up being more influenced by the irrelevant features than the useful ones. This problem, arising with the presence of a large number of irrelevant features, is another case referred to as the *curse of dimensionality* (see section 2.1.1). Nearest neighbours methods are particularly sensitive to this specific example of the curse. This can be partially overcome, however, by weighting each feature differently when calculating distances between instances, or by removing the irrelevant features from the data entirely.

Another issue with the \(k\)-nearest neighbours algorithm is that, because the \(k\) closest training instances to a test instance is only determined upon its presentation for classification, a significant amount of computation might be necessary for each new classification. Many approaches for efficient memory indexing of the training instances have been developed in order to more easily identify the relevant nearest neighbours at the cost of using more memory. An example of such an approach is the *kd*-tree [98, 99], with training instances being stored as leaves in a tree. Instances close to each other are then stored on the same branch or node, making it less computationally intensive to locate the neighbours of a particular instance.
Chapter 2. An Introduction to Machine Learning

An important difference between $k$-nearest neighbours and most other machine learning techniques is the fact that, for each unclassified test instance encountered, $k$-nearest neighbours creates a unique approximation to the target function, whereas most other methods construct approximations that are applied over the whole instance space that is not localised to the neighbouring area of a new test instance. This is a big advantage in cases where the global target function is complex. [93]

Because the $k$-nearest neighbours method is highly unstructured, it is not necessarily of great value when trying to understand the relationships between the feature values and the classification outcome. However, when used as a black-box approach, they often prove to be some of the best-performing algorithms in real-life machine learning problems. [95]

2.2.3 Support Vector Machine

The support vector machine is an example of a maximum margin classifier, which means that the algorithm’s aim is in finding a decision boundary that separates different classes from one another, while also seeking to maximise the separation between them. In the algorithm’s simplest implementation, the decision boundary takes the form of a hyperplane in feature space. Its strength, though, lies in its ability to transform the data features into a higher-dimensional space with the help of the kernel trick (see the next section and Fig. 2.5) where a hyperplane will be more successful in its task of separating classes as well as possible. This then results in a non-linear decision boundary in the original feature space.

In this section, the support vector machine will be discussed by first looking at the case for linearly separable data, then briefly looking at kernel functions (as these are integral to the algorithm) and then considering the case for non-linearly separable data.

2.2.3.1 Formulation of the Support Vector Machine Algorithm

We start off by looking at a binary classification problem making use of linear models with the following form:

\[ y(x) = w^T \phi(x) + b \]  

(2.15)

Here, $b$ is a bias parameter determining the decision surface’s location, $w$ is the weight vector determining the decision surface’s orientation, and $\phi(x)$ is a feature-space transformation. The training set consists of $N$ input feature vectors $x_1, ..., x_N$ having class values $t_1, ..., t_N$, respectively.

\footnote{In $N$-dimensional Euclidean space, a hyperplane is an $N-1$-dimensional flat subset of the space dividing it into two subspaces.}
where \( t_n \in \{-1, 1\} \). New data instances \( \mathbf{x} \) are then classified into one of these two classes depending on the sign of the target function \( y(\mathbf{x}) \), meaning that the decision boundary is defined by the relation \( y(\mathbf{x}) = 0 \).

For now, we’ll assume that the instances in the training data are linearly separable. In other words, there is at least one combination of values of \( \mathbf{w} \) and \( b \) such that Eq. 2.15 satisfies \( y(\mathbf{x}_n) > 0 \) for all training instances having \( t_n = +1 \), and \( y(\mathbf{x}_n) < 0 \) for all training instances having \( t_n = -1 \). We therefore have that \( t_n y(\mathbf{x}_n) > 0 \) for all instances in the training set.

![Figure 2.3: The concept of a margin.](image)

This figure shows a linearly separable training data set with instances belonging to one of two possible classes (shown by the blue and green dots, respectively). The margin is the smallest perpendicular distance between any of the training instances and the decision boundary (shown by the red line at \( y = 0 \)).

It may of course be that there are many solutions for \( \mathbf{w} \) and \( b \) that results in a complete separation of classes for the training data set. In that case, we choose the solution that will result in the smallest classification error when the algorithm is applied to new instances in a validation set. The support vector machine tackles this problem by using the concept of a margin, defined as the smallest perpendicular distance between any of the training instances and the decision boundary, as illustrated in Fig. 2.3.

For a support vector machine, minimising the classification error of new test instances means that the decision boundary is chosen such that the margin is maximised (based on the training data) - from there the saying that it is a maximum margin classifier.

To implement a support vector machine it is necessary to determine the parameters \( \mathbf{w} \) and \( b \) in Eq. 2.15. It can be shown, and is fully derived in Appendix A.1, that this optimisation problem can be reduced to solving
\[ \text{argmin}_{w,b} \frac{1}{2}\|w\|^2, \]

subject to the constraint

\[ t_n(w^T\phi(x_n) + b) \geq 1, \quad n = 1, ..., N \]

where \( n = 1, ..., N \). Because we are faced with having to solve a constrained optimisation problem, we use the Lagrange multipliers\(^3\) \( a_n \geq 0 \), one for each constraint mentioned above, resulting in the Lagrangian function

\[ L(w, b, a) = \frac{1}{2}\|w\|^2 - \sum_{n=1}^{N} a_n \{ t_n(w^T\phi(x_n) + b) - 1 \}, \]

where \( a \) is the vector of Lagrange multipliers. This complex problem is recast in a more tractable form and solved in Appendix A.2, where the values of \( a, w \) and \( b \) are determined.

![Figure 2.4: Maximised margins and support vectors.](image)

When maximising the margin, support vectors (the circled instances) determine the location of the decision surface.

These solutions can be understood intuitively as follows. For every training instance \( x_n \), either \( a_n = 0 \) or \( t_n y(x_n) = 1 \). Instances for which \( a_n = 0 \) will have no influence over the prediction for a new test instance. The remaining training instances, for which \( t_n y(x) = 1 \), are referred to as support vectors and lie on the hyperplanes in feature space corresponding to the maximum margins.

\(^3\)For information on Lagrange multipliers, see Appendix E in Bishop’s book [92].
as is shown in Fig. 2.4. It is therefore important to note that, upon completion of the training phase, only the instances corresponding to the support vectors are retained for the classification of new test instances.

### 2.2.3.2 Kernel Functions

For learning models using a fixed feature space transformation \( \phi(x) \), where \( \phi(x) \) is a vector and \( x \) is its input feature vector, the kernel function is defined as

\[
k(x, x') = \phi(x)^T \phi(x')
\]  

(2.19)

and is a symmetric function of its inputs, such that

\[
k(x, x') = k(x', x)
\]  

(2.20)

Many linear parametric regression and classification models can be reformulated into a dual representation, based on the use of a kernel function evaluated using the training instances. This approach was pioneered by Aizerman et al. in 1964 [100] with applications in pattern recognition, and was rediscovered years later in 1992 by Boser et al. [101], who applied it in a machine learning context that led to the development of the support vector machine algorithm.

Formulating a kernel as an inner product in feature space allows for the use of the kernel trick, saying that if an algorithm has input instances \( x \) entering only as scalar products, the product can be replaced by a kernel to obtain a dual algorithm equivalent to the original. In this way we end up with a dual algorithm expressed entirely with kernels, and can therefore avoid explicitly working with \( \phi(x) \). This allows us the implicit use of feature spaces having higher or infinite dimensionality. To see an example of the application of the kernel trick, see Fig. 2.5.

There are two ways in which a valid kernel function can be constructed. The first is to define a feature mapping \( \phi(x) \) and to then construct a kernel function from that, while the second approach is to construct it directly. In the second case it is necessary to check the validity of the chosen function as a kernel by ensuring that it is a scalar product in some feature space.

However, we need a simpler way of determining whether a kernel is valid without having to determine \( \phi(x) \) explicitly. For this reason we introduce the Gram matrix, denoted by \( K \), a symmetric \( N \times N \) matrix having elements

\[
K_{nm} = \phi(x_n)^T \phi(x_m) = k(x_n, x_m)
\]  

(2.21)
For a kernel $k(\mathbf{x}, \mathbf{x}')$ to be valid, a necessary and sufficient condition \cite{102} is for the Gram matrix to be positive semidefinite\footnote{An $N \times N$ matrix $\mathbf{M}$ is positive semidefinite if $\mathbf{x}^* \mathbf{M} \mathbf{x} \geq 0$, where the column vector $\mathbf{x} \in \mathbb{C}^N$ if $\mathbf{M}$ is complex, or $\mathbf{x} \in \mathbb{R}^N$ if $\mathbf{M}$ is real. Note also that $\mathbf{x}^*$ is the complex conjugate of $\mathbf{x}$.} for all possible sets $\{\mathbf{x}_n\}$. Lastly, new valid kernels can also be constructed by building them using other kernels as building blocks (see the properties in Appendix A.4).

**Figure 2.5:** The kernel trick.

**Left:** Two-class classification with a support vector machine using a linear decision boundary.
**Right:** Two-class classification with a support vector machine making use of the kernel trick.

### 2.2.3.3 Linearly Non-Separable Class Distributions

Up to this point, it was assumed that the training set was linearly separable in some feature space $\phi(\mathbf{x})$, meaning that using a support vector machine will lead to a complete separation of the classes found in the training set in the original input feature space $\mathbf{x}$, where the separation will be done by a non-linear decision surface. In real-life applications, on the other hand, class-conditional distributions often overlap, and finding a complete separation of the classes in the training data is often detrimental to the classifier’s performance on the test set later on.

In order to prevent this overfitting from taking place, the support vector machine needs to be modified in order to allow for the misclassification of some of the instances in the training set. In other words, we now want to allow training instances to fall on the “other side” of the margin hyperplane. To exercise a measure of control over which instances gets misclassified and which don’t, penalties are introduced, implemented through the use of *slack variables* defined as $\xi_n \geq 0$ with $n = 1, \ldots, N$ \cite{103, 104}. Each instance has one slack variable, its value increasing as the distance between the instance and the margin boundary increases. We here take the penalty to be...
a linear function of the aforementioned distance, as this will prove to be most convenient for the optimisation problem we have to solve.

For training instances lying inside or on the correct margin hyperplane, the slack variables are defined as $\xi_n = 0$, while for all other instances they are assigned the value $\xi_n = |t_n - y(x_n)|$. A training instance falling exactly on the decision surface $y(x_n) = 0$ will therefore have a penalty of $\xi_n = 1$, while instances having $\xi_n > 1$ lies at a point on the other side of the decision surface, and will be misclassified. The classification constraint given in Eq. 2.17 for the case of separable classes are therefore replaced with

$$t_n y(x_n) \geq 1 - \xi_n, \quad n = 1, \ldots, N$$

(2.22)

where the penalties are constrained to $\xi_n \geq 0$. Training instances falling on the margin hyperplane or on the correct side of the margin will have slack variables with the value $\xi_n = 0$ and will be classified correctly, as will instances falling between the margin hyperplane and the decision surface on the correct side having slack variables of the value $0 < \xi_n \leq 1$. Instances falling on the decision boundary’s wrong side will have slack variables $\xi_n > 1$, however, and will be misclassified. This is illustrated in Fig. 2.6. This relaxed margin constraint, resulting in what we now refer to as a soft margin, therefore allows for the occasional misclassification of training instances. While this approach allows class distributions to overlap, it remains sensitive to training data outliers due to the fact that the misclassification penalty is linearly increasing with $\xi$.

![Figure 2.6: Slack variables.](image)

This figure shows the slack variables, $\xi_n$, for different support vectors (circled data instances).

Our aim, now, is again to maximise the margin, this time while penalising instances falling inside the margin or on the margin hyperplane itself. This is done by minimising
with respect to $w$, $b$ and $\{\xi_n\}$. As misclassified instances have $\xi_n > 1$, $\sum_N \xi_n$ forms the upper bound to the number of misclassifications. $C$, where $C > 0$, therefore serves as a regularisation parameter that manages the trade-off between the minimisation of errors (the penalties) and the control of the model's complexity (the margin). A low $C$ results in a smooth decision boundary and a high $C$ results in greater classification accuracy. To recover the algorithm used for the case of separable classes, one merely takes the limit $C \to \infty$. We highlight here that the parameter $C$ is user-defined, as is explained later when our particular support vector machine implementation is discussed (section 5.4.3).

We now minimise Eq. 2.23 while taking the constraints in Eq. 2.22 as well as $\xi_n > 0$ into account. Introducing $\{a_n \geq 0\}$ and $\{\mu_n \geq 0\}$ as Lagrange multipliers, we therefore solve the following Lagrangian function:

$$L(w, b, a) = \frac{1}{2} ||w||^2 + C \sum_{n=1}^N \xi_n - \sum_{n=1}^N a_n \{t_n y(x_n) - 1 + \xi_n\} - \sum_{n=1}^N \mu_n \xi_n$$  \hspace{1cm} (2.24)

As before, the solutions for $w$, $b$ and $a$ are given in Appendix A.3.

### 2.2.3.4 Obtaining Probabilistic Outputs

Support vector machines are decision machines, and therefore do not output posterior probabilities for the target values of new test instances. In order to obtain such probabilistic outputs, Platt scaling [105] can be employed - this involves the fitting of a logistic sigmoid, an S-shaped curve defined by

$$\sigma(r) = \frac{1}{1 + e^{-r}}$$  \hspace{1cm} (2.25)

to the outputs of a support vector machine that has already been trained. It is then assumed that the conditional probability we are looking for is as follows:

$$p(t = 1|x) = \sigma(Ay(x) + B)$$  \hspace{1cm} (2.26)
Here, $y(x)$ is defined by Eq. 2.15. $A$ and $B$ can be determined through a maximum likelihood method optimising on a training set that is independent of the training data used for the initial training of the support vector machine so as to avoid over-fitting. In the case where one training set is used for both purposes, an additional cross-validation can be used to avoid over-fitting.

Cross-validation is a technique used for determining how results obtained from a predictive model (in the case of machine learning) will generalise to another, independent set of data. The method uses a fraction $(T - 1)/T$ of the training data for training while systematically employing the whole training set for performance assessment. Consider the case of 4-fold cross-validation ($T = 4$) where the training set has been split into four equally-sized groups, as illustrated in Fig. 2.7. $T - 1$ of these groups are then used for the training of a model, while the remaining group is used for the evaluation of the trained model. This procedure is repeated $T$ times, once for each of the possible choices for the withheld group (indicated with pink in the figure), after which the $T$ performance results are averaged.

2.2.4 Artificial Neural Network

Artificial neural networks have their origin in the study of mathematical representations of biological neural networks [4, 22, 24]. Historically, these algorithms have since been researched by two groups of scientists - the one group, as alluded to above, using neural networks to study learning processes in biological entities; the other group studying them in the pursuit of developing better machine learning methods [93]. For our purposes a biological framework and the corresponding constraints it imposes is of course unnecessary, and this section will therefore concentrate on introducing neural networks in the proper machine learning context by discussing a simple class of networks, called feed-forward network functions, that have shown themselves to be of great value.
Neural networks are nonlinear modelling tools able to approximate target functions that are real-, discrete- or vector-valued. They consist of a system of interconnected nodes, of which each node processes received information before passing it onwards to other nodes using weighted links. These networks can be trained to learn mappings from inputs to outputs, after which it can then use the trained model to make predictions regarding new test data instances. \[88\]

In this section, we discuss artificial neural networks as supervised machine learning algorithms used for the purpose of binary classification. The perceptron, one of the basic units of neural networks, will be discussed first, followed by a description of feed-forward neural networks. Autoencoders, a type of feed-forward network, will be discussed next, after which there will be looked at the training of neural networks. Lastly, we discuss the method of error backpropagation.

### 2.2.4.1 The Perceptron

The perceptron, developed by Frank Rosenblatt \[24\], forms an integral part of the history of artificial intelligence and machine learning in the context of neural networks. The perceptron is a binary classifier that maps an input \(N\)-dimensional feature vector \(\mathbf{x} = (x_1, x_2, \ldots, x_N)\) to either class \(C_1\) or \(C_2\), denoted by the target values \(t = 1\) and \(t = -1\), respectively. \[92\]

The perceptron achieves this by, given the input \(\mathbf{x}\), calculating the target function \(y(\mathbf{x})\) as

\[
y(\mathbf{x}) = \begin{cases} +1 & \text{if } \sum_{i=1}^{N} w_i x_i + w_0 \geq 0 \\ -1 & \text{otherwise} \end{cases}
\]

where \(w_i\), with \(i = 1, \ldots, N\), are real-valued *weights* determining the contribution that each one of the feature inputs \(x_i\) has to the output of the perceptron, and where \(w_0\) denotes a *bias* parameter \[93\]. To simplify notation and for further illustration, see Fig. 2.8, where the feature inputs, weights and bias parameter can be seen on the left, with their sum \(a\) expressed as

\[
a = \sum_{i=1}^{N} w_i x_i + w_0
\]

The function \(h(\cdot)\) is known as the *activation* function, and in the case of the perceptron algorithm is the signum step function. Mathematically, the target function is therefore given by

\[
y(\mathbf{x}) = h(a) = \text{sgn}(a) = \begin{cases} +1, & a \geq 0 \\ -1, & a < 0 \end{cases}
\]
where \( a \) is as shown in Eq. 2.28.

![Figure 2.8: The perceptron.](image)

An illustration of the perceptron classifier, where \( x_i \) and \( w_i \), with \( i = 1, \ldots, N \), denotes the feature inputs and their weights, respectively, and where \( w_0 \) denotes the bias parameter. The weighted sum of the feature inputs is denoted by \( a \) (Eq. 2.28), while \( h \) is referred to as the activation function (see Eq. 2.29).

The perceptron classifier is trained using a set of training instances \( \{x_n\} \) to choose values for the weights \( w_i \). Once training is completed and a reliable mapping between the training inputs and their target values is established, the model can be used for the classification of new test input instances. Because we are primarily interested in feed-forward networks, further details regarding the training of perceptrons is not necessary.

### 2.2.4.2 Feed-Forward Neural Networks

Generally, neural networks can have arbitrary structures, but because a great number of learning applications can be implemented using only feed-forward neural networks [88], it is this type of network that will be discussed in this section. Feed-forward neural networks are the simplest networks and have directed structures - information moves from an input to an output nodal layer via a number of “hidden” node-layers in between [88]. The feed-forward network is often referred to as a multilayer perceptron, even though the simple nodes used in it are not strictly speaking perceptrons (discussed in the above section) in that their activation functions differ. This section discusses the feed-forward neural network algorithm.

For simplicity we consider a 3-layer neural network, shown in Fig. 2.9, consisting of an input layer with \( N \) nodes, a hidden layer with \( M \) nodes and an output layer with \( K \) nodes. Note that the presence of \( x_0 \) and \( z_0 \) in the above figure will be made clear in Eq. 2.36, and can be ignored for now. To determine the hidden layer node outputs, denoted by \( z_j \), we start by constructing \( M \) linear combinations (one for each of the hidden nodes) of the input feature values \( x_1, \ldots, x_N \) of an instance \( x \). This can be expressed in a similar fashion as Eq. 2.28, as
A 3-layer neural network corresponding to Eq. 2.36 showing an input, hidden and output layer, with variables represented by nodes, weights depicted with links, and bias parameters represented by links from the extra parameters $x_0$ and $z_0$, where $x_0 = 1$ and $z_0 = 1$. Information flows in the direction shown by the arrows.

$$a_j = \sum_{i=1}^{N} w_{ji}^{(1)} x_i + w_{j0}^{(1)}$$ \hspace{1cm} (2.30)

with $j = 1, \ldots, M$ and where the superscript $(1)$ means that the parameters are associated with the first network layer. Here, in a similar fashion as in the case with the perceptron, the $w_{ji}^{(1)}$ parameters will be referred to as weights while the $w_{j0}^{(1)}$ parameters will be called biases. The $a_j$ quantities will be referred to as activations, and will be transformed by a nonlinear, differentiable activation function $g(\cdot)^{(1)}$ to give the outputs $z_j$ of the hidden layer nodes. This is as follows:

$$z_j = g^{(1)}(a_j)$$ \hspace{1cm} (2.31)

The nonlinear activation functions used for feed-forward neural networks are usually taken to be sigmoidal, the logistic sigmoid function (on the left in Eq. 2.32) or ‘tanh’ function (on the right in Eq. 2.32) being popular choices. They differ from the perceptron’s activation function in that they are differentiable.
Chapter 2. An Introduction to Machine Learning

\[ g(x) = \frac{1}{1 + e^{-x}} \quad g(x) = \tanh(x) \] (2.32)

To determine the outputs of the nodes in the third layer of the neural network, we next construct \( K \) linear combinations of the \( z_j \) values determined above to obtain the output node activations \( a_k \), as

\[ a_k = \sum_{j=1}^{M} w_{kj}^{(2)} z_j + w_{k0}^{(2)} \] (2.33)

with \( k = 1, \ldots, K \), and where the superscript \( (2) \) indicates that the parameters correspond to the second layer of the network. Again, the \( w_{kj}^{(2)} \) parameters are weights and the \( w_{k0}^{(2)} \) parameters are biases. The output node activations are then transformed with an activation function \( g(\cdot)^{(2)} \) to yield the outputs of the network, \( y_k \), as follows:

\[ y_k = g^{(2)}(a_k) \] (2.34)

Combining these stages, we can write down the overall target function \( y_k(x, w) \) for the 3-layer neural network as

\[ y_k(x, w) = g^{(2)} \left( \sum_{j=1}^{M} w_{kj}^{(2)} g^{(1)} \left( \sum_{i=1}^{N} w_{ji}^{(1)} x_i + w_{j0}^{(1)} \right) + w_{k0}^{(2)} \right) \] (2.35)

with all the parameters for the weights and biases grouped together as \( w \). The neural network algorithm is therefore a nonlinear function mapping the inputs \( x = (x_1, \ldots, x_N) \) to the outputs \( \{y_k\} \) using a vector of adjustable parameters \( w \), where network training is carried out to determine the values of \( w \). To simplify notation we can introduce the extra inputs \( x_0 = 1 \) and \( z_0 = 1 \) so that the bias parameters can effectively form a part of the set of weights. Eq. 2.35 therefore becomes

\[ y_k(x, w) = g^{(2)} \left( \sum_{j=0}^{M} w_{kj}^{(2)} g^{(1)} \left( \sum_{i=0}^{N} w_{ji}^{(1)} x_i \right) \right) \] (2.36)

and is depicted in Fig. 2.9. The 3-layer feed-forward neural network is the most commonly used network structure in practice. This is partly due to the fact that a universal approximation theorem [106] says that any continuous function can be approximated to any given accuracy with a neural network having three or more nodal layers, guaranteed the activation functions are not
polynomials, are piecewise continuous and are locally bounded [88]. Thus a simple 3-layer network
with sigmoidal activation functions, as discussed above, is complex enough to be successfully applied
to most applications.

Choosing the number of hidden nodes in a neural network is an important decision to make. Too
many nodes might lead to overfitting, while too few will result in the network making a sub-optimal
approximation of the target function. Through the use of theoretical considerations [107] and by
looking at empirical evidence [108] it has been found that one hidden layer (as said above) having
$2N + 1$ nodes ($N$ being the amount of inputs) is the optimal neural network structure for the
approximation of continuous functions without the algorithm doing unnecessary work. This is
further supported by the empirical studies carried out by Serra-Ricart et al. [109].

2.2.4.3 Autoencoders

We consider here very briefly a type of feed-forward network called an autoencoder, shown in
Fig. 2.10. The main source of information for this section was the paper by Graff et al. [88] unless
indicated otherwise.

In autoencoders the inputs, denoted in the figure as $x_1, x_2$ and $x_3$, are mapped back to themselves
($x'_1, x'_2$ and $x'_3$) such that the network is essentially trained to approximate the identity function.
An autoencoder typically have more than one hidden nodal layer, and has a central layer about
which the network is symmetrical - this central layer has fewer nodes than either the input or the
output nodal layers. In the figure, the central layer nodes are denoted by $z_1$ and $z_2$, respectively.
Autoencoders can be seen as consisting of two parts: the first part, called the encoder, maps the
input variables to the central layer while the second part, the decoder, maps the central layer
variables to the output layer variables approximating the inputs as well as possible.

The hidden layer variables $z_1$ and $z_2$ are nonlinear functions of the inputs and can be seen as a
reduced set of features. Autoencoders, in fact, can be used in this way for carrying out nonlinear
dimensionality reduction, forming generalisations of methods like principal component analysis
(PCA, see section 2.3.1). It has been shown by Sanger [110] that a single-hidden-layer autoencoder
with linear activation functions is equivalent to PCA.

2.2.4.4 Network Training

A simple method for determining the parameters $w$ of the simple feed-forward neural network is
by minimising the error function

$$E(w) = \frac{1}{2} \sum_{n=1}^{N} \left| y(x_n, w) - t_n \right|^2$$

(2.37)
Figure 2.10: An autoencoder.

The inputs \((x_1, x_2 \text{ and } x_3)\) are mapped to themselves \((x'_1, x'_2 \text{ and } x'_3)\) via a network symmetrical about its central layer (depicted with nodes having the values \(z_1\) and \(z_2\)). \(W_1, W_2, W_1^T\) and \(W_2^T\) are the weights associated with the connections between the different nodal layers.

where \(\{x_n\}\), with \(n = 1, \ldots, N\) is the set of input training feature vectors and where the set \(\{t_n\}\) consists of the corresponding target values. We show in Appendix B.1 how \(w\) is found in iterative steps by making use of the gradient of the error function. In a general case, the computation of the gradient is very expensive - however, in the case of a neural network, the gradient can be readily found via the backpropagation algorithm, which is described in Appendix B.2.

2.3 Feature Extraction

This section discusses principal component analysis (section 2.3.1) and linear discriminant analysis (section 2.3.2) in the context of feature extraction. It should be noted that these sections supply the standard theoretical background in order to provide a basis for understanding later chapters. Discussions and explanations of the methods are kept general, with the specific implementation of each of the algorithms and their deviations from the standard theoretical models discussed in Chapter 4.

2.3.1 Principal Component Analysis

Principal Component Analysis (PCA), also known as the Karhunen-Loève transform, is a technique widely used for tasks such as feature extraction, data compression and dimensionality reduction [92]. The main purpose of PCA is to reduce the dimensions of a data set having many correlated variables in such a way that most of the variance present in the original data set is preserved in
the new set. This is done by orthogonally transforming to a new set of uncorrelated variables, called principal components (PCs), ordered in such a way that the first few PCs contain most of the variance of the original data set [111].

Generally, it is accepted that Pearson (1901) [112] and Hotelling (1933) [113] gave the earliest definitions of PCA [111]. Both of these definitions are still commonly used today and both lead to the same algorithm. Hotelling’s definition is much like the one given in the first paragraph, where a data set is projected orthogonally onto a linear space of lower dimension in such a way that the projected data’s variance is maximised. This new linear space is known as the principal subspace. Pearson, on the other hand, defines PCA as the linear projection minimising the average projection cost, where this cost is defined as the mean squared distance between the original data points and their linear projections. [92]

The standard algebraic derivation of PCA, based on Hotelling’s original definition, will be given in the following section.

### 2.3.1.1 Derivation of PCA – the Maximum Variance Formulation

Let \( \{x_n\} \) be a data set of observations, where \( n = 1, ..., N \) and \( x_n \) is a \( D \)-dimensional Euclidean variable. The aim is to transform, or project, this data onto an \( M \)-dimensional linear space, where \( M < D \), while at the same time maximising the projected data’s variance.

We assume, for now, that \( M \) is known, and start off by projecting the data onto a one-dimensional space (\( M = 1 \)), where the direction of the space is defined by a vector \( u_1 \) of dimensionality \( D \). Because we are only interested in the direction that \( u_1 \) defines and not in its magnitude, we take it to be a unit vector, such that

\[
    u_1^T u_1 = 1. \tag{2.38}
\]

We then project each variable (data point) onto a scalar value as \( u_1^T x_n \), the mean of this projected data then being \( u_1^T \bar{x} \), where \( \bar{x} \) is the data set mean given by

\[
    \bar{x} = \frac{1}{N} \sum_{n=1}^{N} x_n. \tag{2.39}
\]

The variance of the projected data is then

\[
    \frac{1}{N} \sum_{n=1}^{N} \left( u_1^T x_n - u_1^T \bar{x} \right)^2 = u_1^T S u_1 \tag{2.40}
\]
where $S$ is the covariance matrix of the data given by

$$
S = \frac{1}{N} \sum_{n=1}^{N} (x_n - \bar{x})(x_n - \bar{x})^T.
$$

To fully accomplish our goal, we next maximise the projected variance $u_1^T S u_1$, given in Eq. 2.40, with respect to $u_1$. This is done in order to find the direction of projection $u_1$ that would retain most of the variance present in the original data. In order to prevent $\|u_1\| \to \infty$, this maximisation has to be constrained, and we can do that by using the normalisation condition given in Eq. 2.38. In order to enforce this constraint, we use a Lagrange multiplier $\lambda_1$ so that we can then maximise the following:

$$
u_1^T S u_1 + \lambda_1 \left( 1 - u_1^T u_1 \right)
$$

Setting the derivative of Eq. 2.42 with respect to $u_1$ equal to zero and taking the transpose of both sides, we find

$$
S u_1 - \lambda_1 u_1 = 0
$$

or

$$
S u_1 = \lambda_1 u_1.
$$

From Eq. 2.44 it can be seen that $u_1$ is an eigenvector of $S$. Left-multiplying with $u_1^T$ and keeping in mind that $u_1^T u_1 = 1$, we have the following:

$$
u_1^T S u_1 = \lambda_1.
$$

From Eq. 2.45 it can be seen that the projected variance is equal to the eigenvalue $\lambda_1$, and it is therefore evident that in order to maximise the variance we have to set $u_1$ equal to the eigenvector with the largest eigenvalue ($\lambda_1$). This eigenvector is then called the first principal component.

Additional PCs can be defined by each time choosing a new direction (from amongst all the directions orthogonal to those already picked) that maximises the projected variance. In general, for an $M$-dimensional principal subspace, the optimal projection maximising the projected variance.
will be defined by the $M$ eigenvectors $\mathbf{u}_1, ..., \mathbf{u}_M$ of $\mathbf{S}$ corresponding to the $M$ largest eigenvalues $\lambda_1, ..., \lambda_M$. This can be shown using proof by induction, as follows.

If we suppose that the above result holds for an $M$-dimensional principal subspace, an $M + 1$ dimensional projection space will be defined by the $M$ PCs $\mathbf{u}_1, ..., \mathbf{u}_M$ as well as an additional PC $\mathbf{u}_{M+1}$, whose value is to be determined here. In order to ensure that $\mathbf{u}_{M+1}$ is not linearly related to any of the already defined PCs $\mathbf{u}_1, ..., \mathbf{u}_M$, we set the constraint that it should be orthogonal to them (Eq. 2.46), and enforce it with Lagrange multipliers $\eta_1, ..., \eta_M$.

$$
\sum_{i=1}^{M} \mathbf{u}_i^{\top} \mathbf{u}_{M+1} = 0 \quad (2.46)
$$

Following the same arguments as for $\mathbf{u}_1$, we find that the projected variance is now given by $\mathbf{u}_{M+1}^{\top} \mathbf{S} \mathbf{u}_{M+1}$, and we maximise this using the Lagrange multiplier $\lambda_{M+1}$ to enforce the constraint in the form of the normalisation condition given in Eq. 2.47.

$$
\mathbf{u}_{M+1}^{\top} \mathbf{u}_{M+1} = 1. \quad (2.47)
$$

Enforcing the constraints in both Eq. 2.46 and 2.47 using Lagrange multipliers, we now have to find the maximum of the function

$$
\mathbf{u}_{M+1}^{\top} \mathbf{S} \mathbf{u}_{M+1} + \lambda_{M+1}(1 - \mathbf{u}_{M+1}^{\top} \mathbf{u}_{M+1}) + \sum_{i=1}^{M} \eta_i \mathbf{u}_i^{\top} \mathbf{u}_{M+1}. \quad (2.48)
$$

By setting its derivative with respect to $\mathbf{u}_{M+1}$ equal to zero, we obtain the following:

$$
2\mathbf{S} \mathbf{u}_{M+1} - 2\lambda_{M+1} \mathbf{u}_{M+1} + \sum_{i=1}^{M} \eta_i \mathbf{u}_i = 0 \quad (2.49)
$$

By left-multiplying with $\mathbf{u}_{M+1}^{\top}$ and using the constraints for orthogonality, we find that $\eta_j = 0$ for $j = 1, ..., M$. Eq. 2.50 is therefore obtained.

$$
\mathbf{S} \mathbf{u}_{M+1} = \lambda_{M+1} \mathbf{u}_{M+1} \quad (2.50)
$$

From the above equation it can be seen that $\mathbf{u}_{M+1}$ is an eigenvector of $\mathbf{S}$ having eigenvalue $\lambda_{M+1}$. Left-multiplying with $\mathbf{u}_{M+1}^{\top}$ and keeping Eq. 2.47 in mind, we find that, similar to the case with $\mathbf{u}_1$, we have that the projected variance is given by
\[ u_{M+1}^T S u_{M+1} = \lambda_{M+1}, \]  

so that we can attain the maximum variance by selecting \( u_{M+1} \) as the eigenvector having the largest eigenvalue \( \lambda_{M+1} \) amongst those not already chosen. It is therefore seen that the result also holds for principal subspaces of dimensionality \( M + 1 \), completing the inductive step. Seeing as this has already been shown for the case where \( M = 1 \), it follows that the result must hold for any \( M \leq D \).

In summary, PCA involves first finding the mean \( \bar{x} \) of the data set, then evaluating the data covariance matrix \( S \), and finally finding the \( M \) eigenvectors (PCs) of \( S \) corresponding to the \( M \) largest eigenvalues. To extract the features of an instance \( x_n \), it is reconstructed using a linear combination of the \( M \) largest eigenvectors, and the \( M \) corresponding coefficients can then be used as the instance’s new features. Seeing as \( M < D \), \( x_n \) has undergone dimensionality reduction. The \( M \)-dimensional vector of coefficients, also called PC weights, for a specific instance \( x_n \) is denoted by \( a_n \), and can be calculated as

\[ a_n = U^T (x_n - \bar{x}) \]  

where \( U \) is a \( D \times M \) dimensional matrix having the \( M \) largest eigenvectors (PCs) as columns. Here \( a_n \) is now the new feature vector of \( x_n \).

### 2.3.2 Linear Discriminant Analysis

Linear discriminant analysis (LDA) is a technique that can be used for dimensionality reduction - it effectively projects data in the direction that will maximise the variance between respective classes while also minimising variance within classes, leading to greater class separation. The term *linear discriminant analysis* is often used interchangeably with the term *Fisher’s linear discriminant (FLD)* due to the fact that these two methods, in spite of having slightly different derivations, are essentially the same - the difference lying only in that FLD does not make all of the assumptions LDA makes, such as equal class covariances and normally distributed class data. Because the derivation of FLD is more intuitive and explanatory, we will use it in this section - by making the assumptions LDA requires we arrive at the exact same result.

Considering the case of dimensionality reduction for two classes, our goal is to project the \( D \)-dimensional input instance \( x \) to one dimension as follows
\[ y = w^T x \quad (2.53) \]

We can ensure that this data projection maximises the separation of classes by adjusting the elements of \( w \), the weight vector, accordingly. If there are \( N_1 \) data instances in class \( C_1 \) and \( N_2 \) in class \( C_2 \), the two classes have means given by

\[
\begin{align*}
\mathbf{m}_1 &= \frac{1}{N_1} \sum_{n \in C_1} \mathbf{x}_n \\
\mathbf{m}_2 &= \frac{1}{N_2} \sum_{n \in C_2} \mathbf{x}_n
\end{align*}
\quad (2.54)
\]

The easiest way in which to acquire a measure of class separation (when the data is projected on \( w \)), is to look at the separation of the class means of the projected data. We can therefore choose \( w \) such that it maximises

\[ m_2 - m_1 = w^T (m_2 - m_1) \quad (2.55) \]

with

\[ m_k = w^T m_k \quad (2.56) \]

being the mean of the projected instances from class \( C_k \), where \( k \in (1, 2) \) seeing as we are only considering a two-class system. As this expression can grow arbitrarily large if \( w \) is not constrained, we impose that \( w \) be of unit length, such that

\[ \sum_i w_i^2 = 1 \quad (2.57) \]

Introducing a Lagrange multiplier and performing the maximisation, we then have that

\[ w \propto (m_2 - m_1) \quad (2.58) \]

There is a problem with this, though, as is shown on the left of Fig. 2.11. It can be seen here that whereas the two classes are originally well separated, there is considerable class overlap when the data is projected onto a line joining the class means. Fisher’s idea [114] is in maximising a function giving a big separation between the means of the projected classes and a small variance.
in every projected class, in this way minimising the overlap in classes. Eq. 2.53 projects labelled instances \((x)\) to labelled values in a one-dimensional space \((y)\). The projected instances from class \(C_k\) therefore have a within-class variance of

\[
s^2_k = \sum_{n \in C_k} (y_n - m_k)^2
\]

with \(y_n\) given by Eq. 2.53 as \(w^T x_n\). The within-class variance for the entire data set is then just \(s^2_1 + s^2_2\). Next we define the Fisher criterion as the ratio of between-class to within-class variance, as

\[
J(w) = \frac{(m_2 - m_1)^2}{s^2_1 + s^2_2}
\]

and then use Eq. 2.53, 2.56 and 2.59 to rewrite it as

\[
J(w) = \frac{w^T S_B w}{w^T S_W w}
\]

with \(S_B\), the between-class covariance matrix, equivalent to

\[
S_B = (m_2 - m_1)(m_2 - m_1)^T
\]
and $S_W$, the within-class covariance matrix, equivalent to

$$S_W = \sum_{n \in C_1} (x_n - m_1)(x_n - m_1)^T + \sum_{n \in C_2} (x_n - m_2)(x_n - m_2)^T$$

(2.63)

We next differentiate Eq. 2.61 with respect to $w$ and set it equal to zero, after which it is easy to show that $w$ maximises $J(w)$ when it satisfies

$$S_B w = \lambda S_W w$$

(2.64)

where $\lambda$ is an eigenvalue. As we are only interested in the direction of $w$, we note that $S_B w$ has a direction equivalent to that of $(m_2 - m_1)$, leading to

$$S_W w \propto (m_2 - m_1)$$

(2.65)

Multiplying with $S_W^{-1}$, we find

$$w \propto S_W^{-1}(m_2 - m_1)$$

(2.66)

This result can now be used to project the data, using Eq. 2.53, in a way that leads to minimal class overlap. The above gives the exact same result as LDA if we assume that the class covariances are identical and the class data are normally distributed.

### 2.4 Concluding Remarks

The concepts, machine learning algorithms and feature extraction techniques discussed in this chapter supply the necessary theoretical background for later chapters. Background on the naïve Bayes classifier, the $k$-nearest neighbours algorithm, the support vector machine algorithm and artificial neural networks will be necessary for the discussions in Chapter 5, while Chapter 4 will require a knowledge of PCA and LDA.
Chapter 3

Supernova Cosmology

When I had satisfied myself that no star of that kind had ever shone before, I was led into such perplexity by the unbelievable difficulty of the thing that I began to doubt the faith of my own eyes.

— Tycho Brahe

3.1 Introduction

This chapter supplies the reader with the necessary supernova (SN) cosmology background and discusses the data that will be used in later chapters for machine learning purposes. Section 3.2 gives a brief overview of supernova cosmology and the problems associated with the vast amount of data that will be produced by the next generation of transient surveys, while section 3.3 discusses the Sloan Digital Sky Survey II (SDSS-II) SN Survey from which we draw the data used in this thesis. Finally, section 3.4 lays out the machine learning goals of this project, describes the dataset we use to accomplish it and briefly outlines the rest of the chapters in this thesis.

3.2 Supernova Cosmology

Supernovae, first explained in 1934 by Baade and Zwicky [115] following earlier work by Lundmark [116], are among the most violent events in the Universe. They occur at the end of a star’s lifetime, when the star is destroyed by an explosion so powerful that it can briefly outshine an entire galaxy.

SNe are classified based on their spectral features at maximum light [117]. Type I SNe have no hydrogen in their spectra, while Type II SNe have. Type Ib SNe shows prominent helium lines; Type Ic displays neither hydrogen nor helium, and Type Ia SNe have spectra dominated by
lines from higher-mass elements like silicon, sulphur, iron and calcium while lacking hydrogen and helium [118].

Astronomically observed SNe correspond to two very different physical phenomena: the thermonuclear explosion of a naked white dwarf and the core collapse of a star. SNe of class Type Ia are of the thermonuclear type, and occurs in binary systems where two stars, a white dwarf and its companion star, orbit one another. A white dwarf is the latest stage in the evolution of some stars - at this stage, the envelope has been fully expelled and a degenerate core is all that remains of the star. As the companion star enters its red giant phase\(^1\) it starts to inflate and expands beyond its Roche lobe\(^2\), expelling matter that can then be accreted by the white dwarf. The mass of the white dwarf increases until it reaches the Chandrasekhar limit\(^3\) \((\sim 1.4\, M_\odot)\), where \(M_\odot\) denotes solar mass) after which it collapses. This collapse triggers explosive nuclear burning of the white dwarf which completely destroys the entire star, leaving no remnant in its wake.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{crab_nebula.png}
\caption{The Crab Nebula and Crab Pulsar. \textbf{Left:} The Crab Nebula - ejecta from the explosion. Credit: European Southern Observatory (ESO). \textbf{Right:} The Crab Pulsar in the centre of the Nebula that remained after the explosion. This is a superposition of an optical HST image (in red) and a false-colour Chandra x-ray image (in blue). Credit: Arizona State University (ASU), Hubble Space Telescope (HST), National Aeronautics and Space Administration (NASA). [119]}
\end{figure}

Even though Type Ia SNe are thought to be the thermonuclear explosion of a white dwarf, it is not clear that the mechanism under which the white dwarf aggregates mass from a companion star is the only way in which such a star can result in such a SN. The scenario under which two white

\(^1\)All stars are born in the so-called main-sequence, but during their evolution they will leave the main sequence and enter the so-called red giant branch where they eventually become much larger and redder. This happens when a star runs out of hydrogen in its core, causing the core to contract and, as a consequence, its envelope to expand.

\(^2\)In a binary system, the Roche lobe of a star is the region of space where material is gravitationally bound to that star.

\(^3\)The Chandrasekhar limit is the mass beyond which the electron degeneracy pressure in the star cannot stop gravitational collapse. This pressure originates from the Pauli exclusion principle, which doesn’t allow some particles to occupy the same quantum state.
dwarfs merge to produce a Type Ia SN is thought to be a sub-dominant mechanism to produce this type of SN and has been studied in Maoz, Mannucci & Nelemans [120] via simulations which have concluded that at least some Type Ia SNe could come from such a mechanism.

In the standard picture of core collapse SNe, on the other hand, they correspond to the spectral classes Type Ib, Ic and II and occur when the core of a massive star ($M \gtrsim 9 \, M_\odot$, where $M$ denotes the mass of the star) can no longer withstand the gravitational pressure and collapses, releasing enormous amounts of gravitational energy. The imploded core can remain either as a neutron star\(^4\) (usually in the form of a pulsar\(^5\)) or a black hole\(^6\), or it can be entirely destroyed, leaving no remnant. The outcome depends on the initial mass and metallicity of the star [119, 121]. An example of well-known SN remnants are the Crab Nebula and Crab Pulsar shown in Fig. 3.1, remains of the historical SN explosion that was recorded by the Chinese in 1054. Table 3.1 encapsulates the information given above.

**Table 3.1: Characteristics of different types of SNe.**

<table>
<thead>
<tr>
<th>Spectral Type</th>
<th>Ia</th>
<th>Ib</th>
<th>Ic</th>
<th>II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spectrum</strong></td>
<td>No Hydrogen</td>
<td>Silicon</td>
<td>No Silicon</td>
<td>Hydrogen</td>
</tr>
<tr>
<td><strong>Physical Phenomena</strong></td>
<td>Nuclear explosion of low-mass star</td>
<td>Core collapse of evolved massive star (star may have lost its hydrogen or helium envelope during red-giant evolution)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compact Remnant</strong></td>
<td>None</td>
<td>Neutron star (typically appearing as a pulsar), black hole or none.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Light Curve</strong></td>
<td>Standardisable</td>
<td>Large Variations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Although most known SNe can be readily classified as Type Ia, Ib, Ic or II, our knowledge of SNe is by far not complete, and we are discovering and postulating new types of SNe continuously. For example, a non-standard type of SN can arise when two white dwarfs collide, producing a thermonuclear SN [122]. As another example, there has been recent discoveries of superluminous supernovae (SLSN) about 50 times brighter than standard SNe types which are currently poorly studied due to a lack of data and are hence poorly understood. For a review, see [123].

\(^4\)These stars are the smallest (with a radius of roughly 12 – 13 km) and densest stars that we know of - they have a typical mass between $\sim 1.4 \, M_\odot$ and $3 \, M_\odot$.

\(^5\)Pulsars are fast rotating, highly magnetised neutron stars. They emit electromagnetic radiation in a beam, which we detect in periodic pulses as the pulsar rotates. The intervals between pulses are very precise, ranging from roughly seconds to milliseconds for a given pulsar.

\(^6\)A mathematically defined spacetime region having such a powerful gravitational pull that no radiation or particle can escape it.
Whereas there is a lot of variation in the light curves of Types Ib, Ic and II SNe, SNe of class Type Ia are surprisingly standardisable. For an example of how the light-curves of different SN types vary, see Fig. 3.2. The light-curves of Types Ib, Ic and II SNe differ from one-another due to the fact that they depend largely on the mass and metallicity of the progenitor star - and these tend to vary. Type Ia SNe, on the other hand, are typically brighter than Type Ib, Ic and II SNe and have light-curves that are very similar due to the fact that their progenitor stars are roughly identical - these SNe are used as “standard candles” for determining the luminosity distance to cosmological objects. Before discussing these standard candles, it is necessary to take a look at distance measurements in the Universe.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{schematic_light_curves.png}
\caption{Schematic light-curves of SNe.}
\end{figure}

Schematic light-curves (linear in B-magnitude) for SN Type Ia, Ib, II-L, II-P and SN 1987A are shown here. The curve for Type Ib SNe includes Type Ic SNe as well, and represents an average of the two classes. SNe 1979C and 1980K are used for the Type II-L curve, although it should be noted that these may be unusually bright. [124, 125] For more information regarding SNe light-curves, see [126–129].

\subsection{3.2.1 Distance Measurements}

This section looks at the derivation of the luminosity distance. In order to do this, we start by outlining how the metric\footnote{The metric gives the distance in a space between points differing by an infinitesimal coordinate difference $dx_{\mu}$ and controls whether the space is curved or not. $\mu$ is a spacetime direction.} changes in an expanding universe. The Robertson-Walker (RW) metric describes such an expanding, isotropic and homogeneous universe and is given by...
\[ ds^2 = c^2 dt^2 - a(t)^2 \left[ \frac{dx^2}{1 - \kappa x^2/R_0^2} + x^2 d\Omega^2 \right], \]  

(3.1)

where the terms inside the square brackets represent the spatial part of the metric which is being stretched as \( a(t) \), the scale factor, changes. This metric allows non-Euclidean geometry, where \( \kappa = +1 \) if the Universe is closed (spatial sections are 3-spheres), \( \kappa = -1 \) if the Universe is open (spatial sections have hyperbolic geometry), and \( \kappa = 0 \) if the Universe is Euclidean and flat, with \( R_0 \) denoting the radius of curvature. \( d\Omega \) is a solid angle, and corresponds to the angular part of the metric, \( t \) denotes time, \( c \) is the speed of light, \( ds \) is the spacetime distance and \( x \) is the radial comoving distance.

It is convenient and common to make the following coordinate transformation

\[
x = S_\kappa(r) = \begin{cases} 
R_0 \sin(\frac{r}{R_0}) & \text{if } \kappa = +1 \\
r & \text{if } \kappa = 0 \\
R_0 \sinh(\frac{r}{R_0}) & \text{if } \kappa = -1,
\end{cases}
\]

(3.2)

so that the metric can be written as

\[
ds^2 = c^2 dt^2 - a(t)^2 \left[ dr^2 + S_\kappa(r)^2 d\Omega^2 \right]. \]

(3.3)

If we want to calculate the comoving distance between us and an object that has emitted its light at time \( t \) when the Universe had a scale factor of \( a \), we need to integrate the radial part of the metric. The theory of relativity tells us that \( ds \) is equal to zero for the path of a photon. Therefore, if we neglect the angular part of the metric and set \( ds = 0 \), we can write

\[
d_c(a) = S_\kappa \left( \int dr \right) = S_\kappa \left( \int \frac{cdt}{a(t)} \right) \]

(3.4)

where \( d_c(a) \) is the comoving distance. Usually, this integral is written as a function of the Hubble parameter, which is defined as \( H(a) = \dot{a}/a \). The Hubble parameter is what relates the recession velocity of galaxies to the distance of such galaxies from us, and changes as a function of time. The Hubble parameter today is called the Hubble constant \( H_0 \). The parameter can be derived

---

8The scale factor is a multiplicative factor that describes how much the Universe has changed in size from time \( t \) to today.

9Given that Einstein proved that mass bends space, the spatial part of the metric assumes that the Universe can also be curved, hence non-Euclidean.
by writing the solution of Einstein’s equations with the RW metric. This results in the Friedman equation, given below, and depends on the contents of the Universe.

\[ H(a)^2 = H_0^2 \left( \frac{\Omega_m}{a^3} + \frac{\Omega_\kappa}{a^2} + \Omega_\Lambda \right) \]  

(3.5)

In Eq. 3.5 \( \Omega_m \) denotes the ratio of the density of mass in the Universe to the density of mass required for a flat Universe, \( \Omega_\kappa = -\kappa c^2/(R_0 H_0)^2 \) and \( \Omega_\Lambda \) is the ratio of the density of dark energy in the Universe to the density of mass required for a flat Universe. We therefore find

\[ d_c(a) = S_\kappa \left( \frac{c}{H_0} \int \frac{a^{-2} da}{\sqrt{\Omega_m a^{-3} + \Omega_\kappa a^{-2} + \Omega_\Lambda}} \right). \]  

(3.6)

In a non-expanding universe, the comoving distance \( d_c(a) \) and the luminosity distance \( d_L(a) \), which is the distance one can infer by measuring the flux of a source of known luminosity, are the same. In an expanding universe, however, they are not. The energy of photons is decreased by a factor of \( a \) as they are stretched while travelling from their source to us. The rate at which such photons arrive is also decreased by another factor of \( a \) as we are moving away from the source due to the expansion of the universe. Therefore,

\[ d_L(a) = \frac{d_c(a)}{a}. \]  

(3.7)

We have therefore derived the luminosity distance and shown that it depends on the cosmological parameters \( \Omega_m, \Omega_\kappa \) and \( \Omega_\Lambda \).

3.2.2 Type Ia Supernovae as Standard Candles

SNe Ia can be used as standard candles for the determination of the luminosity distance to astronomical objects. Standard candles are objects with very well known absolute magnitudes\(^{10}\) (related to the intrinsic brightness of an object). By comparing such an object’s apparent magnitude with that of its absolute magnitude, its luminosity distance can be calculated.

Let us consider a cosmological source with flux \( F \) and known luminosity \( L \) - the received flux then decreases with distance \( d_L \) from the source as follows

\(^{10}\)The magnitude system is used to indicate the brightness of objects - the larger the magnitude, the fainter the object. A difference of one magnitude is equivalent to a brightness difference of \( \sqrt{100} \). The apparent magnitude of an object is its magnitude as observed from Earth, while its absolute magnitude is the hypothetical apparent magnitude an object would have at a standard luminosity distance of 10 pc.
\[ F = \frac{L}{4\pi d_L^2} \]  

(3.8)

Working with fluxes leads to the concept of an object’s magnitude, as the luminosity distance \( d_L \) of an object can be described in terms of its apparent magnitude \( m \) and its absolute magnitude \( M \), as

\[ \mu = m - M = 5 \log d_L + 25 \]  

(3.9)

The luminosity distance \( d_L \) is here measured in Mpc, and \( \mu \) is the object’s distance modulus. The luminosity distance of an object can therefore be determined if its apparent and absolute magnitudes are known.

**Figure 3.3: Standardisation of SNe lightcurves.**

Light curves of a sample of SNe Ia discovered by the Calan/Tololo Supernova Survey before (left) and after (right) standardisation [130].

SNe Ia can be used as standard candles due to certain assumptions concerning the mass involved in each explosion and the main characteristics of the explosions. As mentioned before, the progenitor stars are all white dwarves in binary systems expected to explode at the Chandrasekhar mass. This similarity in mass results in there being a uniformity in energy released during the supernova explosion, and therefore also a uniformity in intrinsic luminosity (related to the absolute magnitude) of the sources. Even more importantly, a correlation between their decay times and their peak brightness exists, known as the Phillips relation [131–133], allowing us to standardise the sources and greatly reduce the variation within the class of Type Ia SNe. This enables us to very precisely determine their absolute magnitudes which, in turn, reduces the distance moduli (and luminosity
distance) estimation errors for the SNe (see Eq. 3.9). Other corrections to the SN magnitude include correcting for dust extinction as well as transferring the observed flux to the rest frame using a K correction term\textsuperscript{11} [117]. See Fig. 3.3 for an example of this standardisation. [119]

As was seen in Eq. 3.7, the luminosity distance is related to cosmological parameters. Many cosmological models, for example, are fitted to the distance modulus $\mu$, with $\mu$ a function of redshift $z$, in order to constrain their cosmological parameters. Redshift is related to the change in frequency $\nu$ that a photon emitted at a scale factor $a_1$ undergoes up to a scale factor $a_2$, and can be expressed as follows:

$$z = \frac{\nu_1 - \nu_2}{\nu_2} = \frac{a_2}{a_1} - 1.$$  \hspace{1cm} (3.10)

Since $a = 1$ today, we can write down a useful relationship between the redshift of an object observed in the Universe and the scale factor as

$$a = \frac{1}{z + 1}.$$  \hspace{1cm} (3.11)

This section therefore concludes that SNe Ia are excellent cosmological probes. The use of SNe Ia as standard candles by Perlmutter et al. [134] and Riess et al. [135] resulted in the first conclusive evidence of the accelerated expansion of the Universe. This was indicative of the existence of dark energy, and earned them (together with Brian Schmidt) the 2011 Physics Nobel Prize.

### 3.2.3 The Data Deluge

Due to its importance in the constraint of cosmological parameters, supernova cosmology is a well-established field seeing continuous development, with surveys such as the Large Synoptic Survey Telescope (LSST)\textsuperscript{12}, the Dark Energy Survey (DES)\textsuperscript{13}, the Panoramic Survey Telescope & Rapid Response System (Pan-STARRS)\textsuperscript{14} and the Palomar Transient Factory (PTF)\textsuperscript{15} set to produce a vast amount of data in the years to come.

However, such a data deluge will require new statistical inference and machine learning techniques for processing and analysis. The LSST, as an example, will image the entire southern sky every

\textsuperscript{11}A K correction is a redshift- and filter-dependent correction to the magnitude of a given object that arises from the fact that an object’s spectrum is shifted towards the red when the object is at a higher redshift; hence, for a set of objects with the same rest-frame spectrum placed at different redshifts, a given filter will sample different parts of the rest-frame spectrum of each object without this correction.

\textsuperscript{12}http://www.lsst.org
\textsuperscript{13}http://www.darkenergysurvey.org/
\textsuperscript{14}http://pan-starrs.ifa.hawaii.edu/public/
\textsuperscript{15}http://www.astro.caltech.edu/ptf/index.php
night with such frequency and depth that the amount of transient alerts expected each night is more than a million, while on the time-scale of a decade at least a million Type Ia SNe candidates will be detected [136]. Existing spectroscopic follow-up capabilities will be swamped by this amount of data, and we will enter an era where small spectroscopic subsets will be used to train processes of photometric transient identification [137–143]. Such methods will always result in a small number of misidentifications, with the danger being that this contamination, unless dealt with carefully, can lead to biased results.

This vast amount of data creates problems in the analysis pipeline long before the final scientific analysis is reached, however. As an example, consider difference images, produced by the subtraction of a reference image of a certain part of the sky from the latest image of that same area. Ideally, the reference image will consist of pure noise unless a transient like an asteroid, SN or variable star exists in the reference image. In real life, however, instrumental effects (e.g. registration errors, diffraction spikes, bleeding and CCD  saturation) cause the occurrence of artefacts.

It is therefore necessary to be able to distinguish between artefacts and objects that might potentially be of interest. This classification into artefacts and real objects has, historically, been carried out by astronomers scanning the images by hand shortly after they have been taken. For the Sloan Digital Sky Survey (SDSS) SN Survey, this practice lead to hand scanners typically sorting hundreds or thousands of images per night - a very time-consuming job. It has recently been shown that scanning such images by hand can be done quite successfully by crowdsourcing [144] - 93% of the SNe that was spectroscopically confirmed was correctly identified by the public.

Although this success sounds alluring, one should be reminded that using human beings for the purposes of classification introduces great difficulties in quantifying the biases originating from the different internal decision trees and algorithms in the brain of each scanner. Additionally, a scanner’s effective decision tree will vary with time according to tiredness, mood and environment , making it impossible to be characterised systematically. For the SDSS-II SN Survey, the bias introduced by the scanners was partly dealt with by the injection of fake SNe into the system so that an average detection efficiency could be determined for every hand scanner - however, this is very clearly a limitation fundamental to human hand scanning that will be even worse in the case of crowdsourcing. Apart from this, hand scanning will be completely infeasible for surveys like the LSST due to the fact that millions of images will have to be scanned per night.

To succeed in the objectives of future transient surveys, the successful substitution of human hand scanners with machine learning techniques for the purpose of this artefact-transient classification

\[16\] A charge-coupled device (CCD) is a circuit etched onto a surface of silicon that forms light sensitive elements referred to as pixels. Electric charge is generated when photons hit the surface, and this is interpreted and/or manipulated by electronics and digitised.


\[18\] This is a well-known problem that affects even the most experienced practitioners. For example, the verdicts of judges vary strongly depending on the time since the last break [145].
therefore represents a vital frontier. Existing work comprise of work done by the SNfactory [146, 147], where the main object’s shape, FWHM (Full Width at Half Measure) and position, along with the distance to the closest object also contained in the reference image were used as features. The work of the Palomar Transient Factory is also of interest, where the emphasis is on the separation of variable stars and transients [148] and the discovery, by [149], of variability in imaging surveys in the time domain where estimations of the degree to which newly found objects are astronomically relevant objects of variable brightness is output by classifiers in the form of probabilistic statements.

3.3 The Sloan Digital Sky Survey: Supernova Survey

The SDSS began its survey operations in 2000 and has progressed through several phases: SDSS-I (2000-2005), SDSS-II (2005-2008), SDSS-III (2008-2014) and SDSS-IV (2014-). Each of these phases comprised of multiple surveys having interlocking scientific goals.

The original SDSS observing plan that stretched from 2000 to 2008 (consisting of both SDSS-I and II), is known as the SDSS Legacy Survey - it resulted in a well-calibrated, uniform map of the Universe that will be used for scientific studies for decades to come. During the first five years of operation, SDSS-I carried out deep multi-colour imaging over 8000 deg$^2$ and measured spectra of over 700,000 objects. SDSS-II completed the original survey goals of imaging half the northern sky as well as mapping the three-dimensional clustering of 100,000 quasars and a million galaxies. Additional to this, SDSS-II carried out two more surveys: the Supernova Survey and the Sloan Extension for Galactic Understanding and Exploration (SEGUE). The Supernova Survey discovered hundreds of supernovae for the purpose of measuring the expansion history of the Universe, and it is this survey that is of interest to us.

3.3.1 The SDSS-II Supernova Survey

The SDSS-II SN Survey was a three-year project running from 1 September to 30 November each year from 2005 to 2007 with the aim of discovering and producing well-measured light curves of SNe Ia in an intermediate redshift range ($0.05 < z < 0.35$). The survey, using the SDSS telescope located at the Apache Point Observatory in New Mexico, did repeated five-band ($ugriz$) imaging of SDSS Stripe 82, a 300 deg$^2$ area centered on the celestial equator. [150]

The SN Survey was designed to address two main issues: the scarcity of SN Ia data found at intermediate redshifts (often referred to as the “redshift desert”), and the systematic limitations introduced by previous SN Ia surveys. At the time, cosmological constraints were based on a Hubble diagram constructed from low- ($z \lesssim 0.1$) and high-redshift ($z \gtrsim 0.3$) SN Ia samples, observed with a variety of telescopes, photometric passbands and selection criteria - naturally
introducing systematic errors. Obtaining more precise cosmological constraints therefore required more control over the sources of these systematic errors - calling for larger SN samples having continuous redshift coverage of the Hubble diagram that consisted of high-quality, multi-band data with well-understood photometric calibration. [150]

With its large areal coverage, photometric accuracy and sensitivity, the SDSS-II Supernova Survey could find thousands of SNe and transient objects at the intermediate redshift ranges lacking in SN Ia data. What is more, the survey was able to carry out a median of 10 single-epoch exposures per band for SNe, resulting in more detailed light-curve data that further reduced systematic errors. By surveying Stripe 82, it could take advantage of the extensive database of object catalogues, reference images and photometric calibration previously obtained by the SDSS-I for this same region. The uniformity of the instrumentation employed by both these surveys, in conjunction with the fact that both surveys obtained photometric standards from the same telescope, further minimised systematic errors. [150]

3.3.1.1 The Supernova Survey Science Goals

What follows is a short summary of the primary science goals that the SDSS-II SN Survey had, as set out by Frieman et al. [150].

1. **Refining the SN Ia Hubble diagram.** SN Ia distance measurements are required to constrain the history of the Hubble parameter. As the SDSS-II SN Survey was set to obtain distance modulus estimates for SN Ia in the redshift range $0.05 < z < 0.35$, a region that was up to that point sparsely populated on the Hubble diagram, it would provide data leading to the obtaining of information on the evolution of the cosmic scale factor that no other supernova survey could yet supply.

2. **Minimisation of SN systematics.** Because of the fact that, at the time, most SN surveys had systematic errors comparable to their statistical errors, the SDSS-II SN Survey aimed at improving control over systematic errors. The SDSS’s photometric calibration errors are small due to the fact that effort were made over many years on the large-scale calibration of the data [151] - photometric errors of 1% have been achieved over Stripe 82, the area that the SDSS-II SN Survey observed [152]. Furthermore, the $ugriz$ filters used by the SDSS-II SN Survey provided important colour information, and it used a stable, single camera with well-calibrated and well-measured filter transmission curves. The SDSS native magnitudes are also close to the AB system [153], with offsets that are well-measured.

3. **Anchoring the Hubble diagram.** It was estimated that the size and quality of the low-redshift portion ($z \lesssim 0.15$) of the SDSS-II SN Survey, upon completion, would be sufficient
to anchor the Hubble diagram and retrain light-curve fitters. This would reduce the necessity to rely on the heterogeneous low-redshift samples used up to that stage.

4. **Rest-frame ultraviolet light curve templates.** SNe surveys operating in the region \( z > 1 \) must have their SN light curves matched to low-redshift templates in order to reduce systematic errors. As an example, observations made at \( z = 1.2 \) in the reddest optical passbands (~8000 Å) correspond to 3600 Å (the \( u \)-band) in the SN rest-frame. At \( z = 0.3 \), the SDSS would observe this region at 4700 Å, the survey’s \( g \)-band. The SDSS-II SN Survey would therefore be able to improve the rest-frame ultraviolet template data \([154]\) necessary for interpreting high-redshift SNe data.

5. **SN characteristics from multi-band photometry.** Because spectra, which are used to determine SN types and redshifts, are obtainable for only a small amount of possible candidates, the SDSS aimed at improving measures to obtain this same information via other routes. The multi-coloured light curves traced out by SNe Ia as they evolve, in combination with their host-galaxy colours, can provide information on SN type, redshift and age.

6. **SN types, rates and host galaxies.** Apart from spectroscopically confirmed SNe Ia, the survey would also yield light-curves of additional SNe - objects likely to be SNe Ia, but is spectroscopically unconfirmed, as well as other types of SNe. This, in combination with the fact that the detection efficiency was monitored by inserting artificial SNe into the data stream, enabled the survey to obtain more robust measures of SN rates. Furthermore, the SDSS supernova sample would provide a large set of host galaxies whose characteristics can be used to glean information about the progenitor properties (\([155, 156]\)). Lastly, because of the large volume that it covered, the SDSS-II SN survey would serve as a probe for rare and interesting objects.

### 3.3.1.2 Technical aspects of the SN Survey

The SDSS produced photometric measurements in each one of the \( ugriz \) SDSS pass-bands \([157]\) using the 2.5m SDSS telescope \([158]\) and photometric camera \([159]\), covering the wavelength range from 350 to 1000 nm. The \( g, r \) and \( i \) bands are the best-suited for observing SNe, as the \( u \) and \( z \) bands have relatively poor throughput at low redshifts (\( z \lesssim 0.1 \) for SNe Ia). \([160]\)

The SN Survey repeatedly scanned Stripe 82, an area 2.5° wide in Declination that stretches between a Right Ascension of 20\(^{h}\) and 04\(^{h}\), in order to discover new SNe and take measurements of those already discovered. The camera was operated in drift-scan mode. Data in a CCD are read by sequentially shifting it from its current pixel to the pixel directly below until it reaches the end of the CCD where it is read out by external electronics and converted into a usable format. If the speed at which data is shifted in this manner is made equivalent to the speed at which an object in
the sky drifts by in front of the camera due to the Earth’s rotation, the telescope is being operated in drift-scan mode. This enables the telescope to image long continuous strips of the sky.

The SDSS camera contains six columns of CCD chips - each column contains five chips, each with a different filter. The telescope (being operated in drift-scan mode) lets objects in the sky drift across these columns, and the CCD’s are then read out in sync with the drifting. An illustration of the camera can be seen in Figure 3.4 - using the orientation in the figure, a specific region of the sky will drift vertically downward through a single column of the camera (as shown by the long arrows), encountering, in turn, the $r, i, u, z$ and $g$ filters. An object takes 55 seconds to drift across one CCD chip - the exposure time for each passband is therefore 55 seconds. By offsetting the camera slightly to account for the gaps between the columns of CCD chips, full coverage of Stripe 82 could be obtained in two nights, with the average cadence being roughly four nights due to weather effects and moonlight interference.

![Figure 3.4: The SDSS photometric camera.](image)

The camera consists of six columns of CCD chips - each column contains five chips, each with a different filter. Using the configuration in the figure, an object will drift vertically downward through a column (as shown by the arrows), in this way encountering each of the five SDSS filters ($r, i, u, z$, and $g$) in turn.

The $u, g, r, i$ and $z$-band SDSS camera images were processed using the first stages of the SDSS reduction pipeline [161] in order to produce calibrated images to be used as SN search data. Deep, co-added reference images (called templates), created using data taken throughout 2004 during
the SDSS-I Survey, were then subtracted from their corresponding search frames \[162\] to produce difference images for the purpose of SN detection. “Real-time” image subtraction was only carried out in the \(g\), \(r\) and \(i\) bands, as they are most useful for SN detection.

The difference images were next sent through an automated object detection algorithm - objects that were detected in more than one of the three passbands, that didn’t coincide with existing catalogued stars or variable objects and were not determined to be moving during the interval between the \(r\) and \(g\) exposures, were kept for further investigation. In 2005, these selected images were then sent to hand scanners who manually evaluated and classified the objects (see section 3.4.1).

In 2006 and 2007, however, additional software cuts were introduced in order to reduce the amount of images that required manual hand scanning. Now, single-epoch detections were only sent onwards to manual scanners if they were not detected as moving (with an improved algorithm, see \[163\]) and if they were bright enough \((r < 21 \text{ or } g < 21)\)\(^{19}\). Otherwise, detection in at least two epochs were required for an object to be sent for hand scanning. During visual hand scanning, an object was then denoted a “candidate” if it was deemed a possible SN, and some of these promising candidates were then sent for spectroscopic follow-up in order to determine whether they truly were SNe.

### 3.4 Classification Goals and Chosen Dataset

Following on from the big data problems of future surveys and human hand scanner biases discussed in section 3.2.3, the purpose of this thesis is to explore the possibility of successfully replacing human hand scanners in optical SN surveys with machine learning algorithms for the task of distinguishing between artefacts and transient\(^{20}\) objects.

Existing work in this field has been discussed in section 3.2.3. In this thesis, however, we use data from the SDSS-II SN Survey and derive our features from Principal Component Analysis and Linear Discriminant Analysis (PCA and LDA, see Chapter 4) of the Sloan \(g\), \(r\) and \(i\) difference images before comparing a number of different potential machine learning algorithms (see Chapter 5) with one another. The following subsections describe the dataset we use, as well as the classification systems we employed for use in our feature extraction methods and machine learning applications in later chapters.

\(^{19}\)For the SDSS survey rate yielding a 55 second integrated exposure in each of its passbands, a 50% detection completeness is achieved for sources at \(u = 22.5\), \(g = 23.2\), \(r = 22.6\), \(i = 21.9\) and \(z = 20.8\) \[150, 164]\). A source at \(r = 21\) and \(g = 21\) is therefore 1.6 magnitudes brighter in the \(r\)-band and 2.2 magnitudes brighter in the \(g\)-band than the detection threshold stated above.

\(^{20}\)The word “transient” is here meant in an over-arching manner - it applies to all the real objects in our dataset, discussed in section 3.4.1 and further described in Table 3.2. It should not be confused with the similarly-named hand-scanner class discussed in the next section.
3.4.1 Dataset and Classification Systems

The data used in this thesis is taken from the last two years (2006 and 2007) of the SDSS-II SN Survey. Data from 2005 were omitted due to the different threshold cuts employed by the survey at the time (as mentioned in section 3.3.1.2) - we did not want to introduce unnecessary variation from outdated filtering procedures into our dataset. A team of roughly twenty hand scanners using the $g$, $r$ and $i$-band search and difference images (each having a size of $51 \times 51$ pixels) as well as object history data classified each of the candidate objects into one of ten possible classes: dipoles, artefacts, saturated stars, transients, variables, moving objects, SN Gold, SN Silver, SN Bronze and SN Other [150]. Each one of these classes is described [165] in Table 3.2, and Fig. 3.5 depicts a simplified decision tree for the visual classification process followed by the hand scanners. Table C.1 shows different $r$-band object images for each of the above-mentioned classes, and also shows how image quality differ depending on the Signal to Noise Ratio (SNR). Table C.2 shows the $g$, $r$ and $i$-band images of objects from each of the above-mentioned ten classes in order to show how images differ across bands. Our dataset consists of the $g$, $r$ and $i$-band 51 × 51 pixel difference images classified by the hand scanners.

For our feature extraction purposes, we re-categorize the original ten classes into three visual classes, following the observation that some of the classes have visual appearances that are very similar. These three visual classes are: “artefacts”, “real” objects and “dipoles/saturated”, as illustrated in Fig. 3.6. The residuals of real objects are point-like (convolved with the telescope and atmosphere’s seeing), artefacts have residuals resembling diffraction spikes and the residuals of dipoles/saturated objects are often quite point-like, typically with negative flux in some part of the image stemming from saturated CCD effects or registration errors. To see which original classes correspond to which visual classes, see Table 3.2. The visual classification system is used for the extraction of a certain set of features using PCA, as described in Chapter 4.

We are, however, ultimately interested in whether or not we can match the performance of human hand scanners in distinguishing between “real” objects (transients) and “not-real” objects (artefacts and dipole/saturated objects), and these are therefore the classes recognised by our machine learning classifiers - they are trained with object instances classified as either real or not-real. To see the classes corresponding to real and not-real objects, respectively, see Table 3.2.

3.4.2 Training and Testing Protocol

Our full dataset contains 27,480 objects of which 11,959 are not-real and 15,521 are real, where each object is associated with three 51 × 51 pixel images (one from each of the $g$, $r$ and $i$-band). Of these, 2500 objects are fake SNe inserted into the pipeline for the characterisation of the selection...
function and to provide quality control. Our dataset includes the fake SNe to allow for comparison of our results with the performance of humans on the fakes.

Our testing protocol was to sequester 25% of the full data set (referred to as the “test set”) for algorithm comparison after the various classifiers have been trained and have undergone preliminary testing with the remaining 75% of the data. This data split was done before the various classifiers were built and the test set was kept apart from the rest of the data until we were ready for final testing.

Some of our learners can be optimised through the use of cross-validation - 30% of the remaining 75% mentioned above was used as a “validation set” to perform this optimisation while the remaining data, referred to as the “training set”, were used for the training of the classifiers. The grouping of the data for these various purposes can be seen in Fig. 3.7.
Figure 3.6: Visual classification.
Example of the three different visual classes in the $r$-band; (A) shows high-quality images from the real (left), artefact (middle) and dipole/saturated (right) classes - all images here have an SNR above 40; (B) shows more representative images from the real (left), artefact (middle) and dipole/saturated (right) classes - all images here have an SNR below 20, representing roughly 80% of the images in the dataset.

It should be noted here that the initial isolation of the test set is absolutely necessary for an unbiased comparison of our various learners. If the same data is used for the optimisation of an algorithm than for the testing of it there is the danger of “training to the test set”, something that almost certainly will lead to poor results in the real world due to overfitting.

3.4.3 Layout of the Remainder of the Thesis

Now that the necessary background knowledge has been supplied (Chapter 1, 2 and 3) and the objectives of the thesis has been discussed (section 3.4), the remainder of the chapters will be devoted to achieving these objectives. Chapter 4 will discuss the various techniques we employ for feature extraction, while Chapter 5 will detail the training, validation and testing of our five
Figure 3.7: Training, test and validation set.

This diagram shows how the full data set was split for various purposes. The test set was sequestered until the final testing stage, and the remaining data was split into a further training and validation set. The validation set was used for parameter optimisation of certain classifiers.

chosen machine learning algorithms and discuss their results. Finally, our conclusions and avenues of possible future research will be set out in Chapter 6.
Table 3.2: The different classification systems for objects in the dataset.
A description of each of the ten original classes used by the human hand scanners is given [165], and their corresponding visual and main (real/not-real) classification is shown.

<table>
<thead>
<tr>
<th>Original Class</th>
<th>Description</th>
<th>Visual Class</th>
<th>Real/Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artefact</td>
<td>Residuals caused by problems in the image (e.g. diffraction spikes).</td>
<td>Artefact</td>
<td>Not-Real</td>
</tr>
<tr>
<td>Dipole</td>
<td>Residuals with roughly equal amounts of positive and negative flux, caused by errors in image registration.</td>
<td>Dipole/Saturated</td>
<td>Not-Real</td>
</tr>
<tr>
<td>Saturated Star</td>
<td>Residuals of stars that saturate the CCD.</td>
<td>Dipole/Saturated</td>
<td>Not-Real</td>
</tr>
<tr>
<td>Moving</td>
<td>Anything showing signs of motion between cutouts in different passbands.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>Variable</td>
<td>Objects showing a record of long-term variability.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>Transient</td>
<td>Objects with no observation history, no apparent host galaxy in the search image, and no motion.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>SN Other</td>
<td>Objects that are thought to have a good chance of being SNe, but that don’t fit nicely into any of the above classes.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>SN Bronze</td>
<td>Point-like residuals at the centre of their host galaxies - most of the objects in this class later turn out to be either quasars (QSOs), active galactic nuclei (AGN) or foreground variable stars, and not SNe.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>SN Silver</td>
<td>Point-like residuals having no apparent host galaxy - SNe much more luminous than their host galaxies usually fall into this class.</td>
<td>Real</td>
<td>Real</td>
</tr>
<tr>
<td>SN Gold</td>
<td>Possible SNe identified as point-like residuals that are not at the exact centre of their host galaxies.</td>
<td>Real</td>
<td>Real</td>
</tr>
</tbody>
</table>
Chapter 4

Feature Extraction

4.1 Introduction

This chapter discusses the pre-processing applied to the data and the machine learning techniques employed in order to create our various feature sets for training and validation of our machine learning algorithms in Chapter 5. The pre-processing of our data is discussed in section 4.2, while the two machine learning techniques, namely Principal Component Analysis and Linear Discriminant Analysis (PCA and LDA) that we employed for feature extraction is discussed in section 4.3. A summary of our various feature sets are provided in section 4.4. It should be noted that the features for one object alone is referred to as a feature vector, while all the feature vectors for all the objects in a given data set is referred to as a feature set.
4.2 Pre-Processing

The raw data for our classification problem are the values of the pixels for the $51 \times 51$ pixel difference images. This means that, without any image processing or feature extraction, each object (consisting of a $g$, $r$ and $i$-band image) in our data set is represented by 7803 values. However, because the objects in these images are centered, the outer pixels often carry very little distinguishing information compared to the inner pixels. Cutting out insignificant pixels can be beneficial to the classification process as it removes an excess of irrelevant data that can possibly confuse classifiers as well as swamp computational resources.

In order to determine which cropping size would work best for our data, we successively cropped the $N \times N$ pixel images in our training and validation sets to sizes of $N = 11$, $N = 21$, $N = 31$, $N = 41$ and $N = 51$, respectively. We then extracted our 28 different feature sets (see section 4.4) for each of these cases, and proceeded to train and validate our Support Vector Machine (SVM, see section 5.4.3) for each of the various feature sets in each of the five cases. It was found that the $31 \times 31$ pixel images gave the best results for the largest number of feature sets, with the additional benefit of being computationally less time-consuming than the original case of $N = 51$. Fig. 4.1 shows the $g$, $i$ and $r$-band image of an object before and after cropping.

For thoroughness, and to ensure that the $N = 31$ case is also optimal for our remaining four classifiers, feature sets were built using both the cropped ($N = 31$) and the uncropped ($N = 51$) case. This is further discussed in section 4.4. Furthermore, we also tried to align images using rotations and translations - this did not lead to any improvement in classifier performance, however, and was therefore not implemented.

4.3 Feature Extraction

Machine learning methods need, as their input, features representing the particular instances. In principle, the pixel values of the images themselves could be used as features, but this might be impractical. The first issue here is a computational one: as each instance (object) in our data set consists of three $31 \times 31$ pixel images, the feature vector of one instance alone would comprise of 2883 features - a large number. Another issue is that we are working with highly compressible images - if we include all the pixel values of the cropped images we might confuse the classifiers with irrelevant features, as mentioned before. Having too large a feature space also puts us at risk of the curse of dimensionality.

To overcome these difficulties we employed two well-known machine learning algorithms, PCA and LDA, for the extraction of those features that represent the data most faithfully. Using PCA
Chapter 4. Feature Extraction

(Section 4.3.1), we extracted features in two different ways. The first method, referred to as Multi-class PCA, is discussed in section 4.3.1.3 and comprises of carrying out PCA on the full training data set (see Fig. 3.7) while the second method, referred to as Single-class PCA, is discussed in section 4.3.1.4 and is based on carrying out PCA on each of the visual classes in the training set separately. LDA was carried out using the full training set, and is discussed in section 4.3.2.

4.3.1 Principal Component Analysis

This section details how PCA was used to extract features for our data. It discusses the specific algorithm we employed, the input data to the algorithm and the different ways in which we used PCA in order to derive our features, namely Multi-class PCA and Single-class PCA. The theoretical background to this section can be found in section 2.3.1.
4.3.1.1 The Algorithm

The algorithm we employed was taken from work done by Pedregosa et al. [166], who implemented the Probabilistic Principal Component Analysis (PPCA) model from the work of Tipping and Bishop [167].

As was seen in section 2.3.1, the $M$-dimensional feature vector $a_n$ (consisting of PC weights) of a $D$-dimensional instance $x_n$, where $M < D$, can be expressed as

$$a_n = U^T(x_n - \bar{x}) \quad (4.1)$$

where $\bar{x}$ is the average of the data vectors defined by equation 2.39 and $U$ is a $D \times M$ dimensional matrix having the $M$ largest eigenvectors (PCs) as columns. Fig. 4.2 illustrates the working of Eq. 4.1 and shows clearly the PC weights ($a_n$) extracted as features.

![Figure 4.2: PC weights.](image)

This figure shows the case where the three ($M = 3$) largest eigenvectors (each with a bold number at the top to show their rank in magnitude) are used to extract the feature vector $a_n$ of an instance $x_n$ (the "Original image" in the figure). The PC weights $w_1$, $w_2$ and $w_3$ necessary to arrive at an "Approximate image" as close as possible to $x_n$ is calculated by Eq. 4.1 above and constitute the feature vector $a_n$ of $x_n$. In order to use these images in Eq. 4.1 they would of course first have to be expressed in vector format.

One disadvantage of the standard PCA formalism given in section 2.3.1 is the lack of a probability density model and likelihood measure. By deriving PCA from a density estimation perspective (PPCA) one permits its comparison to other density-estimation methods, creates the possibility of
statistical testing and allows the PCA model to be extended to a mix of such models. Using PPCA, 
U is determined by incorporating it with a set of hidden variables which is assumed to be Gaussian 
distributed and represent the weights to the directions corresponding to the columns of U. Using 
this formulation, after marginalising over the hidden variables, we can obtain a maximum-likelihood 
estimator of U, which is the best-estimated matrix of principal axes (rotated and scaled) of the 
data. For more detail regarding PPCA, see Chapter 12.2 in [92].

4.3.1.2 Creating the Input Vectors

In order to computationally obtain the PCs of a set of R training objects I₁, I₂, ⋯, I₉ with the 
algorithm mentioned above, it is first necessary to construct the input data matrix of these objects 
by representing each object Iₙ by its corresponding vector, Γₙ. This is done by expressing each of 
its g, i and r-band N × N-pixel images as vectors, and then concatenating them. If Iₙ−g, Iₙ−i and 
Iₙ−r denotes the g, i and r-band images, respectively, of object Iₙ and are expressed as

\[
I_{n-g} = \begin{bmatrix} g_{1,1} & \cdots & g_{1,N} \\ \vdots & \ddots & \vdots \\ g_{N,1} & \cdots & g_{N,N} \end{bmatrix}, \quad I_{n-i} = \begin{bmatrix} i_{1,1} & \cdots & i_{1,N} \\ \vdots & \ddots & \vdots \\ i_{N,1} & \cdots & i_{N,N} \end{bmatrix}, \quad I_{n-r} = \begin{bmatrix} r_{1,1} & \cdots & r_{1,N} \\ \vdots & \ddots & \vdots \\ r_{N,1} & \cdots & r_{N,N} \end{bmatrix}
\] (4.2)

then their corresponding vectors Γₙ−g, Γₙ−i and Γₙ−r are constructed as follows:

\[
\Gamma_{n-g} = \begin{bmatrix} g_{1,1} \\ \vdots \\ g_{1,N} \\ \vdots \\ g_{2,1} \\ \vdots \\ g_{N,1} \end{bmatrix}, \quad \Gamma_{n-i} = \begin{bmatrix} i_{1,1} \\ \vdots \\ i_{1,N} \\ \vdots \\ i_{2,1} \\ \vdots \\ i_{N,1} \end{bmatrix}, \quad \Gamma_{n-r} = \begin{bmatrix} r_{1,1} \\ \vdots \\ r_{1,N} \\ \vdots \\ r_{2,1} \\ \vdots \\ r_{N,1} \end{bmatrix}
\] (4.3)

The vectors Γₙ−g, Γₙ−i and Γₙ−r are then concatenated to form the objects representative vector 
Γₙ, as follows
Chapter 4. Feature Extraction

\[\Gamma_n = \begin{bmatrix} \Gamma_{n-g} \\ \Gamma_{n-i} \\ \Gamma_{n-r} \end{bmatrix} = \begin{bmatrix} g_{1,1} \\ \vdots \\ g_{N,N} \\ i_{1,1} \\ \vdots \\ i_{N,N} \\ r_{1,1} \\ \vdots \\ r_{N,N} \end{bmatrix}. \quad (4.4)\]

The data matrix \(X\) for the set of \(R\) objects can then be constructed as

\[X = \begin{bmatrix} \Gamma_1 & \Gamma_2 & \cdots & \Gamma_R \end{bmatrix}. \quad (4.5)\]

where the input to the algorithm is \(X^T\).

4.3.1.3 Multi-class PCA

As mentioned before, Multi-class PCA was carried out by doing PCA (with the algorithm discussed in section 4.3.1.1) on the full training data set mixing all classes together (see Fig. 3.7), whereafter a small fraction of the PCs were kept for the purpose of our feature extraction. To derive features, all objects (from both the training, validation and test sets) were expressed in vector form as shown in the previous section, and were then expressed as a linear combination of these PCs, with the coefficients (weights) being kept as the objects’ features (as expressed in Eq. 4.1).

Fig. 4.3a shows the first six PCs of the full training set for the \(r\)-band images. It should be noted that the first PCs in the figure are less noisy than the last ones. The optimum number of PCs to use for feature extraction depends on the specific classifier and is a parameter that we optimised for each of our classifiers by training and validating them with feature sets derived by including either 0, 5, 10, 25, 50, 100 or 200 PCs, respectively (see section 4.4 for a discussion of our different feature sets).

4.3.1.4 Single-class PCA

Another approach we used for feature extraction was to apply PCA separately to each visual class (see Table 3.2) in the training set, resulting in a unique set of PCs per visual class (see Fig. 4.3b,
Figure 4.3: **Principal Component Analysis**

The first six PCA components in the $r$-band of (a) the full training set, (b) the training set objects belonging to the real class, (c) the training set objects belonging to the artefact class and (d) the training set objects belonging to the dipole/saturated class.
To extract the features of an object $I_n$ found in either the training, validation or test set, the object is first expressed in vector form and then reconstructed using the PCs of each visual class in turn, resulting in a reconstructed object associated with the real, artefact and saturated/dipole class denoted by $\tilde{I}_{n(\text{real})}$, $\tilde{I}_{n(\text{art})}$ and $\tilde{I}_{n(\text{sat/dip})}$ respectively. The error per pixel for the object, denoted by $\varepsilon_{n(\text{class})}$ where $\text{class} \in \{\text{real, art, sat/dip}\}$, between each reconstructed object $\tilde{I}_{n(\text{class})}$ and the original object $I_n$ is then calculated by taking the Euclidean distance between them and dividing by the number of pixels in an object, $m$, as is shown in Eq. 4.6.

$$\varepsilon_{n(\text{class})} = \frac{\sqrt{(I_n - \tilde{I}_{n(\text{class})})^2}}{m}$$  \hspace{1cm} (4.6)$$

As each object consists of an $N \times N$ pixel $g$, $i$ and $r$-band image, where $N = 31$, the number of pixels would be equivalent to $m = 3N^2$. It should also be noted that the first 15 PCs from each of the visual classes were used for obtaining the respective reconstructed objects. The three errors $\varepsilon_{n(\text{real})}$, $\varepsilon_{n(\text{art})}$ and $\varepsilon_{n(\text{sat/dip})}$ calculated in this way are then used as features for object $I_n$.

As before, the algorithm for the calculation of the PCs was taken from the work done by Pedregosa et al. [166], and the data matrices for the individual visual classes were constructed in a similar manner as explained in section 4.3.1.2.

### 4.3.2 LDA

The LDA algorithm that we employed for the extraction of features for our data was taken from work done by Pedregosa et al. [166], who based their model on the work of Hastie et al. [95]. We discussed LDA in section 2.3.2 using the intuitive approach of Fisher’s Linear Discriminant (FLD). The method used by Hastie, on the other hand, arrives at the exact same result obtained in section 2.3.2 by fitting a Gaussian density to the class data and assuming that the covariance matrices of all classes are identical. For more detail regarding this method, see Chapter 4.3 in Hastie’s book [95].

LDA was carried out on the full training set. Seeing as objects are classified into one of two distinguishable classes (namely real and not-real), objects in the training, validation and test sets were therefore projected down to one dimension, resulting in only one LDA component being used as a feature for an object (see section 2.3.2). The input data matrix was constructed in a similar manner as explained in section 4.3.1.3, this time also including the classes of the objects (real or not-real).

Whether or not to include the LDA component in the feature vectors of objects depends on the specific classifier and is a parameter that we optimised for each of our classifiers by training and validating them with feature sets that both include and lack the component (see section 4.4).
4.4 Feature sets

After obtaining our features from PCA (namely the PC weights from Multi-class PCA and the reconstruction errors from Single-class PCA) and LDA, we constructed various feature sets with which to train, validate and test our classifiers - we did not want to select one feature set exclusively seeing as some classifiers might be more successful using one feature set than another, and this was still unclear at this stage. Varying the feature sets therefore served as a further method of optimisation for each classifier.

Exactly what the feature vectors in the feature sets comprised of and the manner in which a number of different feature sets were obtained is explained as follows:

- All feature sets included the three reconstruction errors obtained from Single-class PCA.
- The number of PC weights (obtained from Multi-class PCA) included in the sets were varied between 0, 5, 10, 25, 50, 100 and 200.
- Feature sets either included an LDA component or excluded it.
- Feature normalisation\(^1\) was either carried out or omitted.
- For thoroughness, feature sets were either derived from cropped 31 × 31 pixel images or from uncropped images.

<table>
<thead>
<tr>
<th>Cropped</th>
<th>Uncropped</th>
<th>PC weights:</th>
<th>LDA False</th>
<th>LDA True</th>
<th>Normalise False</th>
<th>Normalise True</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 options</td>
<td>7 options</td>
<td>0, 5, 10, 25, 50, 100, 200</td>
<td>X</td>
<td>X</td>
<td>2 options</td>
<td>X</td>
</tr>
</tbody>
</table>

56 feature sets

\(1\) The feature data were normalised so that all features would have a standard deviation equal to 0.5 and a mean equal to zero. This was done for improving the efficiency with which various routines optimised the different learners’ objective functions.
Chapter 5

Machine Learning Classification of Transient Survey Images

I visualize a time when we will be to robots what dogs are to humans, and I’m rooting for the machines.

– Claude Shannon

5.1 Introduction

This chapter discusses the training, validation, testing and performance results of our five machine learning algorithms for the problem of distinguishing between real and not-real objects. The performance measures used are discussed in section 5.2 while the training, validation and testing procedures are set out in section 5.3. The various learning methods we employed, as well as their testing and individual performance results, are described in section 5.4 - we used a Minimum Error Classifier (MEC, section 5.4.1), a Naïve Bayes (NB, section 5.4.2) classifier, a Support Vector Machine (SVM, section 5.4.3), a $k$-Nearest Neighbour (kNN, section 5.4.4) algorithm and an artificial neural network called SkyNet (section 5.4.5). The performance results of these classifiers are then compared, discussed and analysed in section 5.5.

5.2 Performance Measures

For optimisation, validation and testing of our learning algorithms we employed four performance measures often used in classification problems - the accuracy ($A$), precision ($P$), recall ($R$) and $F_1$-score. These measures are defined using the number of true positives ($t_p$), true negatives ($t_n$), false positives ($f_p$) and false negatives ($f_n$) as:
Chapter 5. *Machine Learning Classification of Transient Survey Images* 72

\[
A = \frac{t_p + t_n}{t_p + t_n + f_p + f_n} \quad (5.1)
\]

\[
P = \frac{t_p}{t_p + f_p} \quad (5.2)
\]

\[
R = \frac{t_p}{t_p + f_n} \quad (5.3)
\]

\[
F_1 = \frac{2PR}{P + R} \quad (5.4)
\]

Precisely what these true/false positive/negative values constitute can easily be seen with the help of a confusion matrix (Table 5.1) where each column corresponds to instances in a predicted class, and each row corresponds to instances in an actual (true) class. With the help of Table 5.1 it is clear that true positives (\(t_p\)), for example, correspond to real objects that were correctly classified as real, and false positives (\(f_p\)) correspond to not-real objects incorrectly classified as real. False negatives (\(f_n\)) and true negatives (\(t_n\)) can be explained in a similar fashion. For the classification problem at hand, the positive class corresponds to our real objects, and the negative class corresponds to our not-real objects.

**Table 5.1: A confusion matrix.**

An archetype of a confusion matrix adjusted for our specific problem, where the positive class corresponds to real objects and the negative class to not-real objects. True/false positives/negatives are denoted as \(t_p\), \(t_n\), \(f_p\) and \(f_n\) respectively.

<table>
<thead>
<tr>
<th>Predicted Class</th>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Class</td>
<td>(t_p)</td>
<td>(f_n)</td>
</tr>
<tr>
<td></td>
<td>(f_p)</td>
<td>(t_n)</td>
</tr>
</tbody>
</table>

Eq. 5.1 to 5.3 can be explained in a more intuitive way as follows: accuracy (\(A\)) is the fraction of all instances that was classified correctly, precision (\(P\)) is the fraction of positively classified objects that actually are positive, and recall (\(R\)) is the fraction of actual positive objects that was classified as positive by the classifier. The \(F_1\)-score (Eq. 5.4), with its worst value at zero and its best at 1, can be seen as the weighted average of \(R\) and \(P\).

The specific classification problem at hand usually dictates which particular performance measures should be used for the measurement of classifier success. Accuracy, for example, can be misleading in problems where numbers of negative and positive instances are hugely different - a classifier always predicting “positive” will have a very good accuracy on a data set in which 99% of objects are in the positive class. Because our data consist of two classes (real and not-real) of roughly
similar sizes, the accuracy can be used as a sensible measure. A measure that is (in most cases) somewhat better than accuracy is the $F_1$-score - a measure of a classifier’s accuracy punishing false positives and false negatives equally, but accounting for big class number hierarchies by weighting them with their inverse contribution to the whole data set.

In practical applications, we may be more concerned with false negatives than with false positives, and vice versa. For an example based on our problem, if the number of instances predicted to be real is small enough that humans can easily verify it, it would be preferable to minimise $f_n$ and therefore maximise $R$. On the other hand, if we have too large a data stream making human checking infeasible, preventing the contamination of data might become important and in that case the better choice would be to minimise $f_p$ and maximise $P$.

Because most learning algorithms output an instance’s probability of being in a specific class, the trade-off between false negatives and false positives can be studied systematically. We do this by using a Receiver Operating Characteristic (ROC) curve - a plot displaying a binary classifier’s performance as its discrimination threshold is changed. A ROC curve is produced with the plotting of a classifier’s True Positive Rate (TPR, equivalent to recall) versus its False Positive Rate (FPR) for different threshold values [168]. Eq. 5.5 shows how the FPR, also referred to as the fall-out, can be calculated.

$$\text{FPR} = \frac{f_p}{f_p + t_n}$$

A ROC statistic commonly employed for model comparison in the field of machine learning is the area under the curve (AUC or “Area Under Curve”) - equivalent to the probability of a classifier correctly classifying an instance chosen at random [169]. As the name suggests, the AUC value for a given classifier is determined by integrating the classifier’s ROC curve in order to yield the area under its curve.

For our real/not-real classification problem we chose accuracy and recall as our prime performance measures for the initial validation and optimisation phases of the classifiers. Because our two main classes (real and not-real) have roughly similar sizes, accuracy can be used as a good measure of success, while recall is an appropriate metric for our problem due to the fact that we are more worried about losing real objects ($f_n$’s) than we are about the possible contamination of the set of classified real objects. It will be easy enough for humans to get rid of false positives afterwards. For the final testing stage where the withheld test data are used we quote all of the above measures ($A$, $P$, $R$, the $F_1$-score and the AUC statistic) and also supply the confusion matrix and the ROC

---

1 If, for example, a binary classifier outputs the probability $p$ of an instance being in a certain class, with the instance classified as part of the class if $0.5 \leq p \leq 1$ but classified as the other if $0 \leq p < 0.5$, the discrimination threshold is $0.5$. 

---
curve for each of the classifiers in order to provide a full picture of the results. Classifiers are then ordered from best- to worst-performing based on $A$, $R$ and also the AUC value.

5.3 Training, Validation and Testing Procedures

This section discusses the procedures according to which our learning algorithms were trained, validated and tested using the different data sets described in Fig. 3.7.

In general, all our algorithms were initially trained and validated with all 56 different feature sets (see section 4.4). During this phase the most successful feature set for each classifier was determined and, where necessary, classifier parameters were optimised. The algorithms were then submitted to the final testing phase during which each classifier was tested with the feature set (now taken from the withheld test set) that proved most optimal for it during the initial validation phase mentioned above. The final testing phase of the algorithms yielded their respective final performance results for the real/not-real classification problem.

It should be noted that, even though some classifiers do not strictly require a validation phase, all algorithms were submitted to each of these phases in order to attain a sense of uniformity throughout the process (a fixed phase for feature set determination and a fixed phase for final testing), and because it allowed for continuous comparison between methods throughout all phases. Any exceptions to the general procedure given above will be discussed in the sections detailing the testing of the individual algorithms themselves (see section 5.4).

5.4 Machine Learning Algorithms and their Implementations

This section discusses the implementation, training, validation and testing of each of the five algorithms that we employed for our classification problem, and gives the performance results obtained during final testing for each. It should be noted that even though some results are given here, they are only discussed and compared in section 5.5. Detail on the theoretical working of these algorithms can be found in Chapter 2.

5.4.1 Minimum Error Classification

Minimum Error Classification (MEC) is our most basic classifier. It does not really constitute a machine learning algorithm, and was merely used in order to see what the classification potential of the simplest of classifiers would be and to create a baseline for comparison. We implemented MEC in MATLAB® [170] on a simple laptop computer (Intel Core i7, with a clock speed of 2.4 GHz).
5.4.1.1 The Algorithm

MEC takes as its inputs only the reconstruction error features derived using Single-class PCA (see section 4.3.1.4). It first assigns an input instance $x_n$ to the visual class ($C_{\text{visual}}$) associated with its minimum reconstruction error as

$$C_{\text{visual}} = \arg\min_{\text{class}} (\varepsilon_{n(\text{class})})$$

(5.6)

where $\text{class} \in \{\text{real, art, sat/dip}\}$ and $\varepsilon_{n(\text{class})}$ is the reconstruction error calculated as shown in section 4.3.1.4. This intuitively reflects the logical reasoning that, on average, an instance should belong to the visual class whose PCA reconstruction of it results in the smallest error.

Finally, if the instance’s minimum error corresponds to either the artefact or the dipoles/saturated visual class, it is assigned to the not-real main class, whereas if the minimum error corresponds to the real visual class, the instance will be assigned to the real main class. For a reminder on how the different classification schemes work, see Table 3.2.

5.4.1.2 Testing

MEC is not a machine learning algorithm in the full sense and as such required no training and was directly tested on the withheld test set. Due to the fact that MEC only takes the reconstruction errors as inputs, only 4 of the 56 feature sets mentioned in section 4.4 could be tested on the classifier. The best results were obtained by using a non-normalised feature set derived from cropped $31 \times 31$ pixel images, yielding an accuracy of 84%, a recall of 92%, a precision of 83% and an $F_1$-score of 87%. The corresponding confusion matrix can be seen in Table 5.2.

<table>
<thead>
<tr>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>3559</td>
</tr>
<tr>
<td>Not-Real</td>
<td>754</td>
</tr>
</tbody>
</table>

Table 5.2: The confusion matrix for MEC.

5.4.2 Naïve Bayes

A Naïve Bayes (NB) classifier is a supervised machine learning algorithm, and is used here for our binary classification problem of distinguishing between real and not-real objects. The reader is reminded that the theoretical background required for this section is found in section 2.2.1. I
designed the NB algorithm and implemented it in MATLAB® on a simple laptop computer (Intel Core i7, with a clock speed of 2.4 GHz) - see Appendix D for the code used.

5.4.2.1 The Algorithm

As mentioned in section 2.2.1.2, the NB classifier’s approach to the classification of an input instance $\mathbf{x}$ is given by

$$C_{NB} = \arg\max_{C_m} P(C_m) \prod_i P(x_i|C_m)$$

(5.7)

where $P(C_m)$ is the prior probability of the class $C_m$, $P(x_i|C_m)$ is the conditional probability of $x_i$ given class $C_m$, where $x_i$ is value of the $i$’th feature of the input instance $\mathbf{x}$, and $C_{NB}$ is the class output of the learning algorithm. $C_{NB}$ corresponds to the class $C_m$ with the highest probability of being correct, given the feature values $(x_1, x_2, \ldots, x_N)$ describing the unclassified input instance $\mathbf{x}$.

The training phase of the NB classifier consists of estimating the $P(C_m)$ and $P(x_i|C_m)$ terms - this is done by counting their respective frequencies in the training data. Once training is completed, the algorithm can be used for the classification of new data instances by using the approach in Eq. 5.7. It should be noted that in our case, $C_m \in \{C_{\text{real}}, C_{\text{not-real}}\}$. Using Eq. 5.7, we therefore essentially calculate (for a given input instance $\mathbf{x}$) the probabilities $P(C_{\text{real}}|\mathbf{x})$ and $P(C_{\text{not-real}}|\mathbf{x})$, and assign $\mathbf{x}$ to the class for which this probability is a maximum.

The $P(C_m)$ terms can be very easily estimated merely by determining the fraction of training data instances belonging to the class $C_m$. The $P(x_i|C_m)$ terms, on the other hand, are estimated by binning the training instances belonging to a given class $C_m$ according to each feature, respectively, where the number of equally spaced bins for each feature is calculated such that there is an average of four training data points in each bin.

The probability $P(x_i|C_m)$ for a new unclassified instance $\mathbf{x}$ is then estimated by noting which fraction of the training instances in class $C_m$ lies in the bin associated with the value $x_i$ of the $i$’th feature of $\mathbf{x}$.

5.4.2.2 Testing

The NB classifier was trained and validated (using the data sets shown in Fig. 3.7) with each of the 56 feature sets mentioned in section 4.4. Upon completion of the validation phase, it was found that the best results came from using a non-normalised feature set derived from cropped $31 \times 31$ pixel images consisting of three reconstruction errors and 50 PC weights. When tested on
Chapter 5. *Machine Learning Classification of Transient Survey Images* 77

the withheld test data, this model yielded an accuracy of 77%, a recall of 86%, a precision of 77%
and an $F_1$-score of 81%. The corresponding confusion matrix is shown in Table 5.3.

<table>
<thead>
<tr>
<th></th>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real</strong></td>
<td>3333</td>
<td>550</td>
</tr>
<tr>
<td><strong>Not-Real</strong></td>
<td>998</td>
<td>1993</td>
</tr>
</tbody>
</table>

Table 5.3: The confusion matrix for NB.

5.4.3 Support Vector Machine

A Support Vector Machine (SVM) is a supervised machine learning algorithm, and is used here for
our binary classification problem of distinguishing between real and not-real objects. The reader
is reminded that the theoretical background required for this section is found in section 2.2.3. The
implementation of the SVM algorithm was done with scikit-learn [166] (version 0.16.0), an open
source machine learning library for Python\(^2\) (we used Python 2.7.9), on a simple desktop computer
(with a clock speed of 2.4 GHz).

5.4.3.1 The Algorithm

The algorithm we employed was taken from the work done by Pedregosa et al. [166] - we imple-
mented their SVC class, which, equivalent to what was explained in section 2.2.3, solves the primal
problem of minimising

$$C \sum_{n=1}^{N} \xi_n + \frac{1}{2}||w||^2$$

with respect to $w$, $b$ and $\{\xi_n\}$, where $w$ is the weight vector, $b$ is the bias, $\xi_n$ is the slack variable
of a training instance $x_n$ and $C$ is a regularisation parameter, referred to here as the soft margin
parameter. The above minimisation has to be carried out subject to the constraints

$$t_n y(x_n) - 1 + \xi_n \geq 0$$

$$\xi_n \geq 0,$$

where $t_n \in \{-1, 1\}$ is the target value of $x_n$ and $y(x_n)$ is the target function having the form

\(^2https://www.python.org/\)
Chapter 5. *Machine Learning Classification of Transient Survey Images*

\[ y(x_n) = w^T \phi(x_n) + b \]  \hspace{1cm} (5.11)

where \( \phi(x_n) \) is a feature-space transformation. For more detail regarding the above equations, their parameters and their interpretations, see section 2.2.3 - the above equations are equivalent to Eq. 2.23, A.23, A.26 and 2.15, respectively.

It is necessary to specify the kernel to be used in the implementation, and subsequently our SVM makes use of the Gaussian kernel, also referred to as the Radial Basis Function (RBF) kernel. The kernel is expressed as follows

\[ k(x, x') = \exp(-\gamma \|x - x'\|^2) \] \hspace{1cm} (5.12)

where \( \gamma = 1/2\sigma^2 \), with \( \sigma \) being the Gaussian’s width and \( \|x - x'\|^2 \) is the squared Euclidean distance between \( x \) an \( x' \). This kernel’s associated feature vector is of infinite dimensionality.

For an SVM using a Gaussian kernel, there are two parameters the user has to supply that need optimisation: \( C \) and \( \gamma \). The soft margin parameter \( C \) manages the trade-off between training instance misclassification and decision surface simplicity, with a low \( C \) resulting in a smooth decision boundary and a high \( C \) in greater classification accuracy. The \( \gamma \) parameter, on the other hand, defines the reach of a training instance’s influence, with a low \( \gamma \) indicating a large influence and a high value indicating the opposite. An appropriate choice of values for these two parameters are critical to the performance of the SVM - their optimisation is discussed in section 5.4.3.2.

For the case of binary classification it is possible to employ Platt scaling [105] in order to output the probability of an instance being in a certain class (the full theoretical background to Platt scaling can be seen in section 2.2.3.4, and should be referred to in the case of confusion). This involves the fitting of a logistic sigmoid to an already trained SVM’s outputs, where the sigmoid’s parameters (note Eq. 2.26) can be determined through the use of a maximum likelihood function optimised, in our case, on the same training set that the SVM was trained with. To prevent over-fitting, the algorithm also carries out a further cross-validation on the training set.

For our problem, we employ Platt scaling for the purpose of outputting \( P(\text{real}) \) for every input instance, such that it will be classified as a real object when \( 0.5 \leq P(\text{real}) \leq 1 \) and as a not-real object when \( 0 \leq P(\text{real}) < 0.5 \).
5.4.3.2 Testing

The training phase (using the training set shown in Fig. 3.7) of the SVM was used for the optimisation of the $C$ and $\gamma$ parameters. For each of the 56 feature sets mentioned in section 4.4, $C$ and $\gamma$ were optimised for by using a grid search and $T$-fold cross-validation (see section 2.2.3.4 for detail on cross-validation), where $T = 3$ was used to split the training set into three equally-sized groups. The values of $C$ and $\gamma$ that were explored with the grid search ranged (for both parameters) from $10^{-3}$ to $10^3$ in powers of 10 - this range is suggested by Pedregosa et al. [166]. For each feature set, cross-validation was therefore carried out for each parameter pair in the grid, yielding an averaged accuracy score for each pair, after which the most optimal $C$-$\gamma$ pair could then be selected.

After each feature set’s optimal $C$ and $\gamma$ value have been determined using the training data, each of the 56 models were then validated using their corresponding validation feature sets. It was found that the optimal results came from $C = 1000$, $\gamma = 0.1$ and a normalised feature set derived from cropped $31 \times 31$ pixel images consisting of the three reconstruction errors, 100 PC weights and an LDA component. When tested on the withheld test data, this model yielded an accuracy of 86%, a recall of 90%, a precision of 85% and an $F_1$-score of 87%. The corresponding confusion matrix is given in Table 5.4.

<table>
<thead>
<tr>
<th></th>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>3514</td>
<td>369</td>
</tr>
<tr>
<td>Not-Real</td>
<td>605</td>
<td>2386</td>
</tr>
</tbody>
</table>

5.4.4 k-Nearest Neighbours

This section discusses the use of a $k$-Nearest Neighbours (kNN) algorithm for our supervised binary classification problem of distinguishing between real and not-real objects. The reader is reminded that the theoretical background required for this section is found in section 2.2.2. As for SVM, the implementation of the KNN algorithm was done with scikit-learn [166] (version 0.16.0), an open source machine learning library for Python (we used Python 2.7.9), on a simple desktop computer (with a clock speed of 2.4 GHz).
5.4.4.1 The Algorithm

The algorithm we employed was taken from the work done by Pedregosa et al. [166] - we used their `KNeighborsClassifier` method which, as also explained in section 2.2.2, classifies each input query instance based on a majority class vote among its $k$ nearest neighbours, where the integer value $k$ is user-specified. We optimised for the value of $k$, as is discussed in section 5.4.4.2. We mentioned in Chapter 2 that one can implement weights for the $k$ nearest neighbours so that the neighbours closer to the query instance contribute more to the vote - we chose not to do this, and so our weights are uniform.

5.4.4.2 Testing

The kNN algorithm was trained (using the training set shown in Fig. 3.7) with each of the 56 feature sets mentioned in section 4.4, yielding 56 different models. For each of these models, the optimal value for $k$ was selected by validating a given model using each of the following values for $k$: 5, 10, 15, 20 and 25. Upon completion of the validation phase, it was found that the optimal results came from using $k = 10$ and a normalised feature set derived from cropped $31 \times 31$ pixel images consisting of three reconstruction errors, 50 PC weights and no LDA component. When tested on the withheld test data, this model yielded an accuracy of 89%, a recall of 90%, a precision of 91% and an $F_1$-score of 90%. The corresponding confusion matrix is shown in Table 5.5.

<table>
<thead>
<tr>
<th></th>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>3506</td>
<td>377</td>
</tr>
<tr>
<td>Not-Real</td>
<td>363</td>
<td>2628</td>
</tr>
</tbody>
</table>

5.4.5 Artificial Neural Network - SkyNet

This section discusses the use of an Artificial Neural Network (ANN) for our supervised binary classification problem of distinguishing between real and not-real objects. The reader is reminded that the theoretical background required for this section is found in section 2.2.4. The University College London\(^3\) (UCL) Physics and Astronomy Department’s Splinter computer cluster (Intel, with a clock speed of 2.4 GHz - we used only one core) was used for the implementation of the algorithm.

\(^3\)http://www.ucl.ac.uk/
5.4.5.1 The Algorithm

We employed SkyNet (version 1.1), a well-known ANN training tool created by Graff et al. [88], as our neural network algorithm. SkyNet can train feed-forward neural networks applicable to a wide range of machine learning problems - examples include classification, regression, clustering, dimensionality reduction and density estimation. It also gives the user the option of training an autoencoder (see section 2.2.4.3), a network that maps its inputs back to themselves - such networks are often used for providing a more intuitive way of carrying out non-linear dimensionality reduction. SkyNet further allows the user to train a Recurrent Neural Network (RNN) - a network in which the links between nodal units form a directed cycle in which nodes have feedback connections, allowing the network to display dynamic temporal behaviour. These networks can employ their internal memory for the processing of arbitrary input sequences, and are therefore often used in this capacity.

SkyNet provides the option of using a pre-training algorithm for the obtaining of network parameters (weights and biases) close to the training objective function’s global optimum - an alternative to using an arbitrary initial state from which the training process is started, and a method that can therefore possibly ease the process of training complex networks. Furthermore, SkyNet uses convergence criteria in order to prevent over-fitting. More information on various variants of methods employed by SkyNet for more efficient optimisation of networks can be found in the paper by Graff et al. [88].

It was mentioned in section 2.2.4.2 that a universal approximation theorem [106] states that any continuous function can be approximated to a given accuracy with a neural network having three or more nodal layers, guaranteed the activation functions are not polynomials, are piecewise continuous and are locally bounded [88]. SkyNet uses the logistic sigmoid function (see Eq. 5.13) as the activation function for its hidden layers and therefore satisfies these conditions. We therefore decided to implement a 3-layer feed-forward neural network consisting of an input, hidden and output nodal layer.

\[
g^{(1)}(x) = \frac{1}{1 + e^{-x}}. \tag{5.13}
\]

Section 2.2.4.2 further mentions that one hidden layer (as said above) having \(2N + 1\) nodes (\(N\) being the amount of inputs) is the optimal neural network structure for the approximation of continuous functions without the algorithm doing unnecessary work [107–109]. We decided to follow these guidelines for choosing the number of hidden nodes in our networks as long as it was computationally feasible - in the case of our largest feature set, for example, \(N = 204\), resulting in a very infeasible and large network structure should the \(2N + 1\) rule be followed strictly.
The activation function for SkyNet’s output nodes are shown in Eq. 5.14. SkyNet provides continuous outputs for classification problems, interpreted as the probabilities of an input instance belonging to a specific class. To achieve this, the softmax function (see Eq. B.5) is applied to the output values so that they sum to unity and are non-negative. For our classification problem, two output nodes are used (one for each of our main classes) so that the final outputs they yield, given an input instance $x_n$, are equivalent to $P(C_{\text{real}}|x_n)$ and $P(C_{\text{not-real}}|x_n)$. The instance $x_n$ is then assigned to the class with the maximum probability.

$$g^{(2)}(x) = x. \quad (5.14)$$

In summary, then, we employed a 3-layer feed-forward neural network consisting of an input layer having $N$ nodes (where $N$ is the number of input features), a hidden layer with $2N + 1$ nodes (where feasible) and an output layer consisting of 2 nodes (equivalent to the amount of classes we are trying to distinguish between). Upon running the SkyNet algorithm, the user has to supply information regarding different possible settings: whether the pre-training method should be used, whether or not an autoencoder or RNN should be implemented, whether the input data should be whitened\(^4\) and which parameters to use for the determination of convergence, to name the important ones. Details on how we chose these settings can be found in section 5.4.5.2. Of course, the number of network layers and the nodes in each layer should also be specified by the user.

5.4.5.2 Testing

Preliminary tests using the training and validation data sets (see Fig. 3.7) and a fixed feature set were carried out in order to establish whether our network should be configured as either an RNN or an autoencoder, and whether the pre-training method should be employed. The network was tested once in its standard configuration, with all three these options disabled, after which it was tested once for each of the options enabled in turn. It was found that each of these options, once enabled, did not yield any notable changes in network performance for our specific problem, and it was on this basis that they were thus deemed unnecessary. In fact, enabling the options only served to lengthen the algorithm’s computational running time. It was furthermore decided that the input features to the network would be left unwhitened, seeing as our own feature sets already incorporated such measures, and that the average error-squared of outputs from the network would be used as the measure that SkyNet employs for determining convergence of the network. For more information about these settings, see the paper [88].

After the above-mentioned settings were determined, we trained and validated the neural network algorithm with each of the 56 feature sets mentioned in section 4.4, adjusting each network’s input

\[^4\text{In SkyNet’s context, the normalisation of input data to the network is called whitening.}\]
and hidden nodes in accordance to the number of input features a given feature set had. This resulted in 56 different neural network models. Upon completion of the training and validation phase, it was found that the optimal results came from using a non-normalised feature set derived from cropped $31 \times 31$ pixel images consisting of three reconstruction errors, 200 PC weights and no LDA component. When this model was tested on the withheld test data, it yielded an accuracy of 88%, a recall of 89%, a precision of 90% and an $F_1$-score of 89%. The corresponding confusion matrix is shown in Table 5.6.

For the testing and validation of networks using feature sets with a smaller number of features, the $2N + 1$ rule mentioned before was used for determining the number of hidden nodes in the network. For bigger feature sets (like the optimal feature set determined above), though, that would yield a number of hidden nodes too large to be computationally feasible. For the optimal feature set above, we used 100 hidden nodes (instead of 407), and the algorithm converged after 140 iterations.

<table>
<thead>
<tr>
<th>Table 5.6: The confusion matrix for SkyNet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>Real</td>
</tr>
<tr>
<td>Not-Real</td>
</tr>
</tbody>
</table>

5.5 Results and Analysis

This section summarises, analyses, adds to and compares the classification results obtained in section 5.4. Section 5.5.1 provides the ROC curve for each classifier and discusses the best-performing classifier, section 5.5.2 discusses inter-classifier agreement and section 5.5.3 describes the classifiers’ performance on the different visual classes. Incorrectly classified objects are studied in section 5.5.4, while section 5.5.5 compares our results with the human hand scanners mentioned in Chapter 3. Finally, section 5.5.6 discusses the performance of our classifiers on spectroscopically confirmed SNe.

It should be noted that the results presented here appear in the paper by L. du Buisson et al. [1].

5.5.1 Best-Performing Classifier

This section discusses the ROC curves and “Area Under the Curve” (AUC) values obtained for our five classifiers, after which it compares their performance results and notes the best-performing learning algorithm.

As was mentioned in section 5.2, one needs probabilistic outputs with a well-defined discrimination threshold from a classifier in order to obtain its ROC curve. Our SVM, for example, outputs $P(\text{real})$
for a given input instance, such that it will be classified as a real object when $0.5 \leq P(\text{real}) \leq 1$ and as a not-real object when $0 \leq P(\text{real}) < 0.5$, corresponding to a discrimination threshold of 0.5. SkyNet outputs two probabilities given an input instance: $P(\text{real})$ and $P(\text{not-real})$. These probabilities sum to one, and so the decision as to the classification of an instance is similar to that of the SVM, also with a discrimination threshold of 0.5.

Our other classifiers (MEC, NB and kNN), on the other hand, do not provide us with such convenient outputs: MEC assigns an instance to the class corresponding to the minimum reconstruction error, kNN is based on a majority class vote among nearest neighbours, and the probability-outputs of NB do not sum to one. It is therefore necessary to convert the outputs of these classifiers into measures that can be used in a similar fashion as probabilities could, with well-defined discrimination thresholds.

In the case of MEC, an object is classified based on which class (real or not-real) the minimum reconstruction error corresponds to (as explained in Section 5.4.1). There are three error-values - one for each of the visual classes. If the minimum error corresponds to that of the “real” visual class, the object is classified as real, while if the minimum error corresponds to either the “artefact” or the “dipoles/saturated” visual class, the object is classified as being not-real. For our goal here, we first note that only the error-value corresponding to the minimum error value of the two visual classes (“artefact” and “dipoles/saturated”) effectively matters when deciding whether an object is real or not-real - leaving us with two error-values to work with: one representing the real class and one representing the not-real class. We then create an estimator of the probability of an object being real, $\hat{P}(\text{real})$, as

$$\hat{P}(\text{real}) = 1 - \frac{\varepsilon_{\text{real}}}{\varepsilon_{\text{real}} + \varepsilon_{\text{not-real}}},$$

(5.15)

where $\varepsilon_{\text{real}}$ denotes the error-value corresponding to the real main class, and $\varepsilon_{\text{not-real}}$ is the minimum error-value of the visual classes corresponding to the not-real main class, as explained above. In the default classification case (discussed in Section 5.4.1) where an instance is classified solely based on the minimum error-value, an object will here be classified as real if $0.5 \leq \hat{P}(\text{real}) \leq 1$ and as a not-real object if $0 \leq \hat{P}(\text{real}) < 0.5$, corresponding to a discrimination threshold of 0.5. This discrimination threshold can now be varied from 0 to 1 in order to construct the ROC curve for MEC.

The NB classifier outputs two probability values (that do not sum to one) for our problem: the probability of an input instance belonging to the real class, denoted here as $P(\text{real})$, and the probability of it belonging to the not-real class, denoted here as $P(\text{not-real})$. The instance is assigned to the class yielding the highest of these probabilities. For the goal of converting this scheme to one where we have a well-defined discrimination threshold, we employ a transformation
similar to the one in Eq. 5.15 used for MEC. We rescale the probabilities in such a way that the estimated probability of an object being real, \( \hat{P}(\text{real}) \), is now

\[
\hat{P}(\text{real}) = \frac{P(\text{real})}{P(\text{real}) + P(\text{not-real})}.
\] (5.16)

In the default classification case (discussed in section 5.4.2) where an instance is classified solely based on the class yielding the highest probability \( P \), an object will here be classified as real if \( 0.5 \leq \hat{P}(\text{real}) \leq 1 \) and as a not-real object if \( 0 \leq \hat{P}(\text{real}) < 0.5 \), corresponding to a discrimination threshold of 0.5. This threshold can now be varied for the purposes of constructing a ROC curve.

In the case of kNN, an instance is classified based on the majority class vote of its \( k \) nearest neighbours. This can very simply be adjusted to our goals merely by introducing an estimator of the probability of an object being real, \( \hat{P}(\text{real}) \), as

\[
\hat{P}(\text{real}) = \frac{k_{\text{real}}}{k_{\text{real}} + k_{\text{not-real}}},
\] (5.17)

where \( k_{\text{real}} \) is the number of real nearest neighbours, \( k_{\text{not-real}} \) is the number of not-real nearest neighbours, and \( k_{\text{real}} + k_{\text{not-real}} = k \). In the default classification case (discussed in section 5.4.4) where an instance is classified solely based on a majority class vote, an object will here be classified as real if \( 0.5 \leq \hat{P}(\text{real}) \leq 1 \) and as a not-real object if \( 0 \leq \hat{P}(\text{real}) < 0.5 \), corresponding to a discrimination threshold of 0.5. This threshold can now be varied for the construction of a ROC curve.

The ROC curves for each of our five classifiers were constructed by using the outputs each of them obtained on the test data and varying their respective discrimination thresholds between 0 and 1 in order to see how their performance with regard to the TPR and FPR changed. The AUC statistic (see section 5.2) for each classifier was also calculated - the ROC curves for the classifiers as well as their respective AUC values can be seen in Fig. 5.1.

Table 5.7 summarises the classification results of the various classifiers on the test set (most of these results were also given in section 5.4), and orders them from best-performing to worst-performing with respect to recall, accuracy and the AUC value. This table, along with Fig. 5.1, represents some of the main results of this thesis. It is interesting that kNN, a very basic nonparametric learner, yielded the best results for all performance measures apart from recall, followed closely by SVM and SkyNet. Interestingly, our simplest classifier, MEC, yielded the best results for the recall measure. For small FPR values, though, Fig. 5.1 shows that its TPR lagged significantly. The differences in results between the best-performing classifiers (kNN, SkyNet and SVM) are very small and better optimisation of these learning algorithms could almost certainly result in a change
Figure 5.1: ROC curve for the various classifiers.
The ROC curve and Area Under Curve (AUC) for each of the five classifiers. The AUC is indicated in brackets next to each classifiers name, and classifiers are listed in order from best-performing to worst-performing, based on the AUC statistic. It should be noted that changing the threshold value of kNN, for example, can easily result in a recall (true positive rate) of 96% with only a slight penalty in the false positive rate - an encouraging sign.

in the final ordering obtained and shown in Table 5.7. From the viewpoint of substituting human hand scanners, the fact that multiple algorithms performed this well is very encouraging.

5.5.2 Inter-Classifier Agreement

For an idea of the inter-classifier agreement with regard to incorrectly and correctly classified objects, we make use of the Cohen’s Kappa coefficient $\kappa$ [172]. This statistical measure of the agreement between two classifiers is thought to be more accurate than a basic percent agreement calculation, seeing as it also takes chance agreement into account. For two classifiers each classifying $N$ instances into one of $K$ mutually exclusive classes, the Cohen’s Kappa coefficient $\kappa$ is determined as

$$\kappa = \frac{P(a) - P(b)}{1 - P(b)}.$$  \hspace{1cm} (5.18)

Here, $P(a)$ denotes the observed relative agreement while $P(b)$ denotes the hypothetical probability of chance agreement. To illustrate how $P(a)$ and $P(b)$ are calculated, consider the following
Table 5.7: Results table.
A summary of the performance results of the various classifiers on the validation data, ordered from best-performing (top) to worst-performing (bottom) based on accuracy (A), recall (R) and the AUC value. The best result for each performance metric is indicated in bold red. The true labels are on the vertical side of the confusion matrices, and the predicted labels are on the horizontal side (see Table 5.1).

<table>
<thead>
<tr>
<th>ML Technique</th>
<th>AUC</th>
<th>A</th>
<th>R</th>
<th>P</th>
<th>F1</th>
<th>Confusion Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>k-Nearest Neighbours (kNN)</td>
<td>0.94</td>
<td>0.89</td>
<td>0.90</td>
<td>0.91</td>
<td>0.90</td>
<td>Real 3506 Not-Real 377</td>
</tr>
<tr>
<td>SkyNet</td>
<td>0.94</td>
<td>0.88</td>
<td>0.89</td>
<td>0.90</td>
<td>0.89</td>
<td>Real 3461 Not-Real 422</td>
</tr>
<tr>
<td>Support Vector Machine (SVM)</td>
<td>0.93</td>
<td>0.86</td>
<td>0.90</td>
<td>0.85</td>
<td>0.87</td>
<td>Real 3514 Not-Real 369</td>
</tr>
<tr>
<td>Minimum Error Classification (MEC)</td>
<td>0.90</td>
<td>0.84</td>
<td>0.92</td>
<td>0.83</td>
<td>0.87</td>
<td>Real 3559 Not-Real 324</td>
</tr>
<tr>
<td>Naïve Bayes (NB)</td>
<td>0.80</td>
<td>0.77</td>
<td>0.86</td>
<td>0.77</td>
<td>0.81</td>
<td>Real 3333 Not-Real 550</td>
</tr>
</tbody>
</table>

example: two classifiers each having to classify each of the objects in the same set as being either real or not-real. This scenario is depicted in Table 5.8, where A and B denote the classifiers, data on the diagonal slanting left shows the count of agreements and the data on the diagonal slanting right shows the count of the disagreements between the classifiers. Here we have \(N = 100\) and \(K = 2\).

Table 5.8: Example classification results.
An example of the classification results of two fictional classifiers, A and B, that both classified each one of 100 objects into one of two classes (real or not-real).

<table>
<thead>
<tr>
<th></th>
<th>Real</th>
<th>Not-Real</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td>40</td>
</tr>
</tbody>
</table>
In Table 5.8, note that there were 40 objects classified as not-real by both classifier A and B, and 30 objects that were denoted as real by both classifiers. The observed relative agreement $P(a)$ is then calculated as

$$P(a) = \frac{40 + 30}{100} = 0.7. \quad (5.19)$$

To calculate $P(b)$, we note that classifier A classified 60 objects as not-real and 40 objects as real - in other words, in 60% of cases it classified an object as not-real, and in 40% of cases it classified an object as real. In 50% of cases, B classified objects as not-real. The probability of both A and B classifying an object as not-real is therefore $0.6 \times 0.5 = 0.3$, while the probability of both classifying an object as real is $0.4 \times 0.5 = 0.2$. The overall probability of chance agreement is therefore

$$P(b) = 0.3 + 0.2 = 0.5. \quad (5.20)$$

Applying Eq. 5.18 for Cohen’s Kappa $\kappa$ we then find

$$\kappa = \frac{P(a) - P(b)}{1 - P(b)} = \frac{0.7 - 0.5}{1 - 0.5} = 0.4. \quad (5.21)$$

If the two classifiers are in perfect agreement, $\kappa = 1$, whereas $\kappa = 0$ when classifiers have no agreement between them apart from that which is expected by chance alone. There are different opinions as to the precise interpretation of the value of $\kappa$ (see, for example, the guidelines by Fleiss et al. [173], Altman [174] and Landis & Koch [175], respectively), but a rough idea of such interpretations can be found in Table 5.9, as put forth by Landis & Koch [175].

**Table 5.9: Interpretation of the Cohen’s Kappa value.**

Guidelines to the strength of agreement between two classifiers based on the value of the Cohen’s Kappa coefficient $\kappa$, as outlined by Landis & Koch [175].

<table>
<thead>
<tr>
<th>Kappa Statistic</th>
<th>Strength of Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\kappa \leq 0.00$</td>
<td>None</td>
</tr>
<tr>
<td>$0.00 &lt; \kappa \leq 0.20$</td>
<td>Slight</td>
</tr>
<tr>
<td>$0.20 &lt; \kappa \leq 0.40$</td>
<td>Fair</td>
</tr>
<tr>
<td>$0.40 &lt; \kappa \leq 0.60$</td>
<td>Moderate</td>
</tr>
<tr>
<td>$0.60 &lt; \kappa \leq 0.80$</td>
<td>Substantial</td>
</tr>
<tr>
<td>$0.80 &lt; \kappa &lt; 1.00$</td>
<td>Almost Perfect</td>
</tr>
<tr>
<td>$\kappa = 1.00$</td>
<td>Perfect</td>
</tr>
</tbody>
</table>
Fig. 5.2 gives the $\kappa$-values for all pairs of our various classifiers (MEC, NB, SkyNet, kNN and SVM) for their performance during final testing. From Fig. 5.2 it can be seen that NB and SVM, and NB and MEC, have a stronger agreement (“moderate”) between them than any of the other pairs of classifiers have. The fact that none of the best-performing classifiers are in strong agreement is a good indication that combining different classifiers’ predictions in an ensemble classifier might yield improved classification results.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{figures/cohen_kappa.png}
\caption{Cohen’s Kappa.}
\end{figure}

The Cohen’s Kappa coefficient ($\kappa$) value for each pair of classifiers, which measures the overlap in performance between classifiers relative to pure chance (which corresponds to $\kappa \leq 0$). These results can be interpreted with the aid of Table 5.9.

5.5.3 Classifier Performance on Different Visual Classes.

Our classifiers’ performance on the respective visual classes (dipoles/saturated, artefacts and real) in the test data set can be seen in Table 5.10. For the recall value calculations here, the true positives ($t_p$) are associated with objects belonging to a specific visual class that were correctly classified as being either not-real or real, while false negatives ($f_n$) are associated with incorrect classifications.

For all of our five learning algorithms the performance on artefacts and real objects is better than the performance on dipoles/saturated objects, the latter class therefore being responsible for the lowering of the overall performance of our algorithms. A possible reason behind the poor classification results for this class comes from the observation that dipoles/saturated and real objects can have quite similar features (compare the PCs in Fig. 4.3d with the ones shown in...
Table 5.10: Classifier performance on visual classes.
The recall of the classifiers on the different visual classes of images. The true positives, \( t_p \), for a class correspond to the images in that class that were correctly classified, and \( f_n \) corresponds to the images that were incorrectly classified. Recall here has the same meaning as accuracy.

<table>
<thead>
<tr>
<th>Visual Class</th>
<th>kNN</th>
<th>SkyNet</th>
<th>SVM</th>
<th>MEC</th>
<th>NB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>0.90</td>
<td>0.89</td>
<td>0.90</td>
<td>0.92</td>
<td>0.86</td>
</tr>
<tr>
<td>Artefact</td>
<td>0.93</td>
<td>0.92</td>
<td>0.90</td>
<td>0.90</td>
<td>0.82</td>
</tr>
<tr>
<td>Dip/Sat</td>
<td>0.79</td>
<td>0.76</td>
<td>0.62</td>
<td>0.47</td>
<td>0.38</td>
</tr>
</tbody>
</table>

Fig. 4.3b), something that can very likely confuse classifiers. Seeing as many dipoles/saturated objects resemble real objects quite closely, and seeing as real object features are (therefore) very well-represented in the PCs we use for feature extraction, noisy dipoles/saturated objects are very easily misclassified as being real - the noise in their images often result in the loss of their distinctive characteristics, leaving them to appear very similar to noisy real objects.

5.5.4 Incorrectly Classified Images

To form an idea of possible reasons behind object misclassifications, we investigated objects that all five of our learning algorithms classified incorrectly. Fig. 5.3 displays three real objects classified as not-real by all classifiers while Fig. 5.4 displays three not-real objects classified as real by all classifiers.

Fig. 5.3a shows an object having a dim point-like residual in the centre of each of its three images - these dim residuals are the reasons for the “real” label of the object, as they are an indication of the object possibly being a SN. This object’s misclassification probably has to do with the fact that all of its images contain a bright dipole-like structure in the top right corner - as we did not restrict the classifiers to only focus on the central pixels of the images, this would be a confusing factor to them. Both of the real objects shown in Fig. 5.3b and 5.3c have dipole-like residuals in all three of their passbands, leaving no mystery as to why all five classifiers mistook them for not-real objects. Originally, the “real” label of the two objects might even have been a mistake made by the human hand scanners, emphasising how erroneous labels can eventually influence the test results.

Fig. 5.4a shows a similar problem, where hand scanners assigned an object to the artefact class that the learning algorithms understandably classified as a real object seeing as there are point-like structures present in all three of its bands. Fig. 5.4b shows an artefact with all three of its images containing masked areas, resulting in the loss of its characteristic spike-like residuals. The remaining point-like residual in the central area of its \( i \)-band image is probably the reason behind it being misclassified as real by all five classifiers. Fig. 5.4c shows a dipole object, as is
Figure 5.3: Real objects classified as not-real.

Examples of objects classified as real by the human hand scanners but classified as not-real by all five machine classifiers. For each object the $g$-band (top), $i$-band (middle) and $r$-band (bottom) image is shown: (a) the dipole-like residuals in the top corner outshining the faint point-like structures probably resulted in misclassification; (b&c) the dipole-like structures observed in the centre of these real object images probably resulted in their misclassification.

made evident to us by the dipole-like structures present in its $i$ and $r$-band images. The noisy nature of the object’s images is possibly what caused all five classifiers to misclassify it as a real object. Furthermore, as was discussed in section 5.5.3, it is often the case that objects from the dipoles/saturated and real class share quite similar features - a possible contributing factor to the object incorrectly being classified as real.

5.5.5 Comparison with Human Classifiers.

As was mentioned in section 3.4.2, fake SNe were injected into the SDSS-II SN survey’s pipeline in order to test hand scanner efficiency. The recall performance on the fake SNe, averaged over all the hand scanners, was $0.956 \pm 0.010$ \cite{176}. For the purpose of comparison, the classification results of our five learning algorithms on the mock SNe in our test data set can be found in Table 5.11. It is clear that three of our classifiers (KNN, SkyNet and MEC) yielded results on the fake SNe that were as good as, or even better than, the average hand scanner recall. Upon inspection of Fig. 5.1, it can furthermore be seen that varying the discrimination threshold and suffering only minor penalties (larger FPR) can result in a recall (TPR) of 96%, even in the case where all test data are used.
Chapter 5. *Machine Learning Classification of Transient Survey Images*  

---

**Figure 5.4:** Not-real objects classified as real.  
Examples of objects classified as not-real by the human hand scanners that were each classified as being real by all five machine classifiers. For each object the $g$-band (top), $i$-band (middle) and $r$-band (bottom) image is shown: (a&b) these artefacts were probably misclassified due to the fact that they appear more point-like than spike-like; (c) the noisy images of this dipole probably resulted in its misclassification.

**Table 5.11:** Performance comparison with humans.  
A summary of the performance results of our five classifiers on the fake SNe found in the test set. The results that are equal or better than that obtained by the human hand scanners are in red.

<table>
<thead>
<tr>
<th>Learning Algorithm</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNN</td>
<td>0.96</td>
</tr>
<tr>
<td>SkyNet</td>
<td>0.96</td>
</tr>
<tr>
<td>SVM</td>
<td>0.94</td>
</tr>
<tr>
<td>MEC</td>
<td>0.96</td>
</tr>
<tr>
<td>NB</td>
<td>0.90</td>
</tr>
</tbody>
</table>

---

**5.5.6 Performance on Spectroscopically Confirmed SNe**

Our classifiers’ performance on the set of spectroscopically confirmed SNe found in our test data set can be seen in Table 5.12 - our test set contained 135 SNe that were spectroscopically confirmed, of which 110 were SNe Ia and the remaining 19 were comprised of other SNe types (type Ib, Ic and II).

It can be seen that MEC, SVM, SkyNet and kNN yielded good results, with a minimum recall value of 0.90 amongst them - an echo of earlier successes. The weakest learning algorithm of the group continues to be the NB classifier, with a maximum recall value of 0.76 for the case of spectroscopically confirmed Type Ia SNe.
Table 5.12: **Classifier performance on spectroscopically confirmed SNe.**

The recall of the various classifiers on the 135 spectroscopically confirmed SNe in the test set (110 SNe Ia and 19 other SNe). The first row shows the performance on the group of SNe Ia, while the second row details the results for the other 19 SNe (excluding SNe Ia). The last row shows the classification results for all 135 spectroscopically confirmed SNe together.

<table>
<thead>
<tr>
<th></th>
<th>kNN</th>
<th>SkyNet</th>
<th>SVM</th>
<th>MEC</th>
<th>NB</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN Ia</td>
<td>0.94</td>
<td>0.92</td>
<td>0.90</td>
<td>0.91</td>
<td>0.83</td>
</tr>
<tr>
<td>SNe</td>
<td>1.00</td>
<td>1.00</td>
<td>0.89</td>
<td>1.00</td>
<td>0.63</td>
</tr>
<tr>
<td>All</td>
<td>0.95</td>
<td>0.93</td>
<td>0.90</td>
<td>0.93</td>
<td>0.80</td>
</tr>
</tbody>
</table>

5.5.7 **Classifier Run Time Considerations**

The computational run time for training and testing each of our five classifiers with their respective best-performing feature sets, along with the various machines used for their implementation, can be seen in Table 5.13.

It can be seen that, with the exception of SkyNet, all run times were on the order of mere seconds or minutes. SkyNet’s long training time (~18 h) might appear to be disadvantageous, but when keeping in mind that classifier training is carried out only once and that thereafter the real-time classification of new objects can take place indefinitely, this becomes an insignificant once-off payment in time. It is therefore the testing time of the classifiers that is of lasting importance - in our case all classifiers classified the 6874 objects in the test set in seconds or minutes. It should be noted that this same task would take a human hand scanner days to complete.

Table 5.13: **Classifier run times.**

The training and testing run times for our various classifiers on their respective best-performing feature sets, along with the machines on which they were implemented. Note that MEC does not require any training (see section 5.4.1.2). The desktop computer had a clock speed of 2.4 GHz, the laptop computer had an Intel Core i7 2.4 GHz processor and the cluster was an Intel 2.4 GHz, of which only one core was used (see section 5.4.5).

<table>
<thead>
<tr>
<th></th>
<th>Training time</th>
<th>Testing time</th>
<th>Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>kNN</td>
<td>~20 s</td>
<td>~35 s</td>
<td>Desktop computer</td>
</tr>
<tr>
<td>SkyNet</td>
<td>~18 h</td>
<td>~1 s</td>
<td>Computer cluster</td>
</tr>
<tr>
<td>SVM</td>
<td>~1.5 min</td>
<td>~10 s</td>
<td>Desktop computer</td>
</tr>
<tr>
<td>MEC</td>
<td>N/A</td>
<td>~3 s</td>
<td>Laptop computer</td>
</tr>
<tr>
<td>NB</td>
<td>~6 s</td>
<td>~1.5 min</td>
<td>Laptop computer</td>
</tr>
</tbody>
</table>
Even in the unlikely case where machine classifiers and humans take the same amount of time to classify new objects accurately, it would still be advantageous to have the job done by a machine - not only does it enable the human scanner to do other important tasks that can not be automated, but it also ensures that any classification results are reproducible and that human classification biases are avoided. Apart from this, hand scanning will be completely infeasible for surveys like the LSST due to the fact that millions of images will have to be scanned per night.
Chapter 6

Conclusions and Future Work

The search to find answers to the deepest questions we have about the Universe has fueled the collection of data for ever larger volumes of our cosmos. The field of supernova cosmology, for example, is seeing continuous development due to its importance in constraining cosmological parameters, with surveys such as the LSST, DES, Pan-STARRS and the PTF set to produce a vast amount of data that will require new statistical inference and machine learning techniques for processing and analysis.

This vast amount of data creates problems in the analysis pipeline of such SN surveys - when we consider difference images, for example, they should ideally consist of pure noise unless a transient exists in the reference image. In real life, however, instrumental effects cause the occurrence of artefacts, and it is therefore necessary to be able to distinguish between artefacts and objects that might potentially be of interest. This classification into artefacts and real objects has, historically, been carried out by astronomers scanning the images by hand shortly after they have been taken.
In the case of the SDSS-II SN Survey, this practice lead to hand scanners typically sorting hundreds or thousands of images per night. This method of classification has two very apparent problems. The first is the issue of time - assigning humans to a task such as this is very time-consuming, and would be a completely infeasible approach to classification for the large upcoming surveys mentioned above. The second issue is that human classifiers introduce great difficulties in quantifying the biases originating from the different internal decision trees and algorithms in the brain of each scanner.

To succeed in the objectives of future transient surveys, the successful substitution of human hand scanners with machine learning techniques for the purpose of this artefact-transient classification therefore represents a vital frontier. In this thesis we explore this prospect by testing various leading machine learning algorithms and showing that many of them can match the human hand scanner performance in classifying transient imaging data from the SDSS-II SN survey into real objects and artefacts.

In Chapter 2, we introduce the field of machine learning, an area of research concerned with the creation of computer programs that can improve their performance on a given task through experience. We start by discussing the important concepts used in the discipline and describe the three major learning categories that machine learning applications most commonly belong to: supervised, unsupervised and reinforcement learning. In this thesis we are interested in supervised classification, having as its goal the assignment of an input instance to one of a number of mutually exclusive classes, using training sets consisting of both the features and the class values of the training instances. We next supply the theoretical background for the machine learning algorithms and the feature extraction techniques that we employ in later chapters: we discuss the Naïve Bayes (NB) classifier, the $k$-Nearest Neighbours (kNN) algorithm, the Support Vector Machine (SVM) algorithm and Artificial Neural Networks (ANNs) as classification algorithms, and Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) as feature extraction techniques.

Chapter 3 introduces SN cosmology - it describes the main categories of SNe and discusses the importance of using Type Ia SNe as standard candles for the constraining of cosmological models. The chapter also discusses the data deluge expected from upcoming SN surveys, addresses the limitations and problems introduced by using human hand scanners for artefact/real classification (as mentioned above) and proposes the substitution of human classifiers with machine learning algorithms. It then proceeds to give an outline of the science goals and technical aspects of the SDSS-II SN Survey, after which it describes the data we draw from it for our classification purposes, the classification systems we employ, the splitting of our data into a training, validation and a withheld test set and our classification goal - to match the performance of the SDSS human hand scanners in distinguishing between real objects (transients) and not-real objects (artefacts, dipoles and saturated stars).
In Chapter 4 we discuss the pre-processing and feature extraction techniques applied to our data in order to produce the various feature sets we employ for classification purposes in Chapter 5. We carry out PCA on each one of our visual classes in the training set individually in order to obtain a set of PCs for each visual class - these PCs can then be used to reconstruct a test object for the purpose of calculating its reconstruction error features. PCA was also carried out on our full training set in order to obtain a set of PCs for the extraction of PC weights from test objects. Finally, we applied LDA to our training data for the purpose of calculating an LDA component for each test object. By varying the number of PC weights, by either including or omitting the LDA component, by either normalising the features in the feature set or leaving them non-normalised, and by extracting features from either $31 \times 31$ or $51 \times 51$ pixel images, a total of 56 different feature sets were obtained with which to optimise our various classifiers with.

In Chapter 5 we start off by discussing the performance measures we use for judging the classification results of our learning algorithms - accuracy, recall, precision, the $F_1$-score and the AUC value. We then proceed to discuss the training, validation and testing procedures for our classifiers. In general, all our algorithms are initially trained and validated with all 56 different feature sets. During this phase the most successful feature set for each classifier is determined and, where necessary, classifier parameters are also optimised. The algorithms are then submitted to the final testing phase during which each classifier is tested with the feature set (now taken from the withheld test set) that proved most optimal for it during the training and validation phase. The chapter next discusses the implementation and the training, validation and final testing of each of our five classifiers: a very simple method referred to as Minimum Error Classification (MEC), a kNN and SVM algorithm obtained from the work of Pedregosa et al. [166], an ANN algorithm, SkyNet, obtained from the work of Graff et al. [88] and an NB classifier.

The classification results are then summarised, compared and analysed. After additionally obtaining ROC curves and AUC values for all five classifiers, it is found that kNN, a very basic nonparametric learner, is the best-performing classifier for our problem with regard to accuracy (89%), recall (90%) and the AUC value (94%), our chosen measures for final performance evaluation. SkyNet and SVM follow closely behind. A study of inter-classifier agreement is next conducted, and it is found that none of the best-performing classifiers (kNN, SkyNet and SVM) are highly correlated in their classifications, an indication that combining different classifiers’ predictions in an ensemble classifier might yield improved classification results. Classifier performance on the different visual classes is investigated next, and it is found that all five classifiers perform better on artefacts and real objects than on dipoles/saturated objects. The latter class is therefore responsible for the lowering of the overall performance of our algorithms. We also discuss objects that were incorrectly classified by all our classifiers, and speculate as to the possible reasons why that might have happened - original mislabelling by the hand scanners, masking and noise obscuring the distinctive features of objects and the presence of other objects in images confusing the classifiers are considered. When comparing our results with those of the human hand scanners on
the set of fake SNe in our test data, it is seen that three of our classifiers (kNN, SkyNet and MEC) match their recall performance of \(\sim 96\%\), meaning that our goal of matching human performance is achieved. We then investigate the algorithms’ performance on the spectroscopically confirmed SNe in the test set, and find that all our classifiers (apart from NB) yielded excellent results, with kNN yielding the highest recall value of 95%. Finally, the various training and testing run times of our classifiers are discussed - it is found that, with the exception of SkyNet’s training time of \(\sim 18\) h, all other run times were on the order of mere seconds or minutes, much faster than human hand scanners would be able to accurately classify the same data sets.

This thesis opens many possible avenues for future research. By also including the search images of objects in the classification process (and not only making use of difference images), we will have access to the host galaxy information of objects - information that might improve classification performance. It might also prove useful to include information on the history of objects. We are currently able to match human hand scanners by using only difference images, while the hand scanners themselves had access to difference and search images as well as object history - it would be interesting to compare our results once we make use of the extra information they employ. More possibilities for research include the use of multi-epoch data for classification and the combination of algorithms into an ensemble classifier (as mentioned above) to investigate the possibility of any further improvements in the classification performance. With all the above information added to the classification process, it would also be interesting to investigate the possibility of distinguishing between different subclasses of transients.

The use of machine learning algorithms for data processing, classification and analysis in astronomy is going to play a role of ever-increasing importance as the amount of data we work with increase. Our future ability to effectively use large repositories of data may depend largely on how effective our machine learning capabilities are - making this an important, challenging and rewarding problem to solve in the coming years.
Appendix A

Mathematical Background on Support Vector Machines

Introduction

This appendix contains additional information and derivations related to the support vector machine algorithm, discussed in section 2.2.3. The main source is [92].

A.1 Derivation of Support Vector Machine Constraints for Linearly Separable Training Data

Following from section 2.2.3.1, we are looking for solutions resulting in the correct classification of all training instances, and therefore have $t_n y(x_n) > 0$ for all $n$. It can be shown that the perpendicular distance between a point $x_n$ and the decision boundary can be given as

$$r = \frac{y(x)}{||w||}. \quad (A.1)$$

By using

$$y(x) = w^T \phi(x) + b, \quad (A.2)$$

defined in section 2.2.3.1, we can therefore write Eq. A.1 as
Appendix A. Mathematical Background on Support Vector Machines

\[
\frac{t_n y(x_n)}{||w||} = \frac{t_n (w^T \phi(x_n) + b)}{||w||}. \tag{A.3}
\]

Seeing as the margin is defined to be the smallest perpendicular distance between the decision boundary and any instance \(x_n\) in the training data set, and seeing as we want to maximise the margin with respect to \(w\) and \(b\), we have to solve the following:

\[
\argmax_{w,b} \left\{ \frac{1}{||w||} \min_n \left[ t_n (w^T \phi(x_n) + b) \right] \right\} \tag{A.4}
\]

It should be noted that \(w\) is not dependent on \(n\). Finding a direct solution to Eq. A.4 is very complex, and so we try instead to find an equivalent problem that we can solve more easily. We see that when the two parameters \(w\) and \(b\) are rescaled such that \(w \rightarrow \beta w\) and \(b \rightarrow \beta b\), the distance between the decision boundary and any instance \(x_n\), given by Eq. A.3, remains unchanged. This allows us to set

\[
t_n (w^T \phi(x_n) + b) = 1 \tag{A.5}
\]

for the instance \(x_n\) closest to the decision boundary, resulting in all training instances satisfying the constraints

\[
t_n (w^T \phi(x_n) + b) \geq 1, \quad n = 1, \ldots, N \tag{A.6}
\]

referred to as the decision hyperplane’s canonical representation. This has been taken into account in Fig. 2.3. For data instances for which the equality in Eq. A.6 holds, the constraints are referred to as being active, while for the rest of the instances the constraints are said to be inactive. Seeing as there is always an instance closest to the decision hyperplane, there is always one active constraint at least, and two active constraints if the margin is maximised. Taking the above into account, we now only need to maximise \(||w||^{-1}\) in order to solve Eq. A.4. Seeing as this is the same as minimising \(||w||^2\), we are simply left with having to solve

\[
\argmin_{w,b} \frac{1}{2} ||w||^2, \tag{A.7}
\]
while taking into account the constraints set out in Eq. A.6. This is now a quadratic programming problem. The inclusion of the 1/2 factor in Eq. A.7 will be made clear later. It might appear that $b$ is not part of the optimisation problem any longer, but it is in fact now just implicitly determined by the constraints, requiring that when changes are made to $||w||$ it is compensated by changing $b$.

### A.2 Determination of Support Vector Machine Parameters for Linearly Separable Training Data

Following from section 2.2.3.1, because we are faced with having to solve a constrained optimisation problem, we use the Lagrange multipliers $^2 a_n \geq 0$ (one for each constraint in Eq. A.6), resulting in the Lagrangian function

$$L(w, b, a) = \frac{1}{2}||w||^2 - \sum_{n=1}^{N} a_n \left\{ t_n (w^T \phi(x_n) + b) - 1 \right\} \quad (A.8)$$

Here, $a = (a_1, ..., a_N)^T$ - it should also be noted that we are here minimising with respect to $b$ and $w$ while maximising with respect to $a$. By taking the partial derivative of Eq. A.8 with respect to $b$ and $w$, and setting those relations equal to zero, these two conditions are obtained:

$$w = \sum_{n=1}^{N} a_n t_n \phi(w_n) \quad (A.9)$$

$$0 = \sum_{n=1}^{N} a_n t_n \quad (A.10)$$

By replacing $w$ and $b$ in Eq. A.8 with the above two relations, we find the maximum margin problem’s dual representation, shown in Eq. A.11. This then has to be maximised with respect to $a$:

$$\tilde{L}(a) = \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m k(x_n, x_m) \quad (A.11)$$

This maximisation will be carried out subject to a set of constraints, shown in Eq. A.12 and A.13:

---

1 A quadratic programming problem is one in which we try to optimise a quadratic objective function while taking certain linear inequality constraints into consideration.

2 For information on Lagrange multipliers, see Appendix E in Bishop’s book [92].
\[ a_n \geq 0, \quad n = 1, \ldots, N \tag{A.12} \]
\[ \sum_{n=1}^{N} a_n t_n = 0. \tag{A.13} \]

In Eq. A.11, the kernel function is defined by

\[ k(x, x') = \phi(x) \phi(x') \tag{A.14} \]

as noted earlier in section 2.2.3.2. This optimisation problem is again an example of a quadratic programming problem.

If a quadratic programming problem has \( M \) variables, it generally requires a solution with computational complexity \( O(M^3) \). In transforming the original optimisation problem in Eq. A.7 into the dual problem in Eq. A.11, we have moved from minimising over \( M \) variables to maximising over \( N \) variables, where \( M \) is the number of fixed basis functions and \( N \) is the number of training data instances. It may appear that the change to the dual problem is disadvantageous when looking at situations where \( M \) is smaller than \( N \). However, it allows a reformulation that makes use of kernel functions, enabling the classifier to be applied successfully to feature spaces having dimensionality larger than the number of training instances \( N \). This holds even for feature spaces having infinite dimensionality. The formulation given above further also clarifies the purpose of the constraint specifying the positive definiteness of the kernel function \( k(x, x') \) (see section 2.2.3.2), as it causes the Lagrangian function \( \tilde{L}(a) \) to be bounded below.

The sign of \( y(x) \) (given by Eq. A.2) is evaluated for the classification of new input test instances when the training phase is completed and the model determined. To express this in terms of the kernel function and the parameters \( \{a_n\} \), we use Eq. A.9 to substitute for \( w \) in Eq. A.2 in order to obtain

\[ y(x) = \sum_{n=1}^{N} a_n t_n k(x, x_n) + b. \tag{A.15} \]

It can be shown that a constrained optimisation of the form shown in Eq. A.15 satisfies the Karush-Kuhn-Tucker (KKT) [177, 178] conditions (see section A.5). In the case of our problem, this means that the optimisation of Eq. A.15 requires the following constraints to hold:
From this it can be seen that for every \( x_n \), either \( a_n = 0 \) or \( t_n y(x_n) = 1 \). In the latter case, instances are support vectors (defined in section 2.2.3.1). Having established a value for \( a \) by solving the problem in Eq. A.11, we now want to determine \( b \)'s value. By keeping in mind that the relation \( t_n y(x_n) = 1 \) holds for any support vector, substituting for \( y(x) \) using Eq. A.15 we have that

\[
t_n \left( \sum_{m \in S} a_m t_m k(x_n, x_m) + b \right) = 1,
\]

where \( S \) is the set of support vector indices. Instead of determining \( b \) through the use of a random support vector \( x_n \), we rather focus on a solution that is more stable numerically. This is done by multiplying both sides of Eq. A.19 with \( t_n \) (noting that \( t_n^2 = 1 \)) and then taking the average of the equations over the entire set of support vectors. Finding \( b \) then results in Eq. A.20, where the support vectors' total number is denoted by \( N_S \).

\[
b = \frac{1}{N_S} \sum_{n \in S} \left( t_n - \sum_{m \in S} a_m t_m k(x_n, x_m) \right).
\]

### A.3 Determination of Support Vector Machine Parameters for Linearly Non-Separable Training Data

Following from section 3.2, we need to solve for the following Lagrangian function

\[
L(w, b, a) = \frac{1}{2} ||w||^2 + C \sum_{n=1}^{N} \zeta_n - \sum_{n=1}^{N} a_n \{t_n y(x_n) - 1 + \zeta_n\} - \sum_{n=1}^{N} \mu_n \zeta_n,
\]

where \( \{a_n \geq 0\} \) and \( \{\mu_n \geq 0\} \) are Lagrange multipliers, subject to the KKT conditions.
Appendix A. Mathematical Background on Support Vector Machines

\[ a_n \geq 0 \quad (A.22) \]
\[ t_n y(x_n) - 1 + \zeta_n \geq 0 \quad (A.23) \]
\[ a_n(t_n y(x_n) - 1 + \zeta_n) = 0 \quad (A.24) \]
\[ \mu_n \geq 0 \quad (A.25) \]
\[ \zeta_n \geq 0 \quad (A.26) \]
\[ \mu_n \zeta_n = 0 \quad (A.27) \]

with \( n = 1, \ldots, N \). Substituting \( y(x) \) in Eq. A.21 for its definition, given in Eq. A.2, and setting the partial derivatives of the Lagrangian with respect to \( w, b \) and \( \{\xi_n\} \) equal to zero, the following is obtained:

\[
\frac{\partial L}{\partial w} = 0 \Rightarrow w = \sum_{n=1}^{N} a_n t_n \phi(x_n) \quad (A.28)
\]
\[
\frac{\partial L}{\partial b} = 0 \Rightarrow \sum_{n=1}^{N} a_n t_n = 0 \quad (A.29)
\]
\[
\frac{\partial L}{\partial \zeta_n} = 0 \Rightarrow a_n = C - \mu_n \quad (A.30)
\]

Eq. A.28, A.29 and A.30 is then used for the purpose of eliminating \( w, b \) and \( \{\xi_n\} \) in Eq. A.21 to obtain its dual representation, shown in Eq. A.31.

\[
\tilde{L}(a) = \sum_{n=1}^{N} a_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{m=1}^{N} a_n a_m t_n t_m k(x_n, x_m) \quad (A.31)
\]

Although this looks similar to Eq. A.11, the difference lies in the constraints it is subject to. Firstly, noting Eq. A.30 and the Lagrange multiplier \( \mu_n \geq 0 \), it can be seen that \( a_n \leq C \). Further taking into account the fact that \( a_n \) is also a Lagrangian multiplier and therefore constrained to \( a_n \geq 0 \), we find that Eq. A.31 should be minimised with respect to \( \{a_n\} \) while taking the constraints

\[
0 \leq a_n \leq C \quad (A.32)
\]
\[
\sum_{n=1}^{N} a_n t_n = 0 \quad (A.33)
\]

into account, where \( n = 1, \ldots, N \). Eq. A.32 are called box constraints. As before, this is a quadratic programming problem. By substituting Eq. A.28 into Eq. A.2, it is found that, as
Appendix A. Mathematical Background on Support Vector Machines

before, classifications for new test data are made through the use of Eq. A.15, given again here for convenience.

\[ y(\mathbf{x}) = \sum_{n=1}^{N} a_n t_n k(\mathbf{x}, \mathbf{x}_n) + b \]  

(A.34)

As before, we note that training instances having \( a_n = 0 \) will play no role in the above model, with the rest of the instances being the support vectors with \( a_n > 0 \). Using Eq. A.24, the support vectors must therefore satisfy

\[ t_n y(\mathbf{x}_n) = 1 - \zeta_n \]  

(A.35)

When \( a_n < C \), it can be seen from Eq. A.30 that \( \mu_n > 0 \). This, together with Eq. A.27, means that the slack variables must therefore be of value \( \xi_n = 0 \), meaning that instances with such a value of \( a_n \) will fall on the margin itself. Instances having \( a_n = C \) can fall inside the margin and can either be correctly classified or misclassified based on whether the value of the slack variable is \( \xi_n \leq 1 \) or \( \xi_n > 1 \), respectively.

Lastly, to find the bias \( b \) in Eq. A.2, we remark that for support vectors having \( 0 < a_n < C \), the slack variables are \( \xi_n = 0 \). Substituting this into Eq. A.35 gives

\[ t_n y(\mathbf{x}) = 1 \]  

(A.36)

and subsequently substituting for \( y(\mathbf{x}) \) using Eq. A.15 and noting that only support vectors have any influence on the predictive model, we can write

\[ t_n \left( \sum_{m \in S} a_m t_m k(\mathbf{x}_n, \mathbf{x}_m) + b \right) = 1 \]  

(A.37)

By averaging to get a stable solution, as before, we find that

\[ b = \frac{1}{N \mathcal{M}} \sum_{n \in \mathcal{M}} \left( t_n - \sum_{m \in S} a_m t_m k(\mathbf{x}_n, \mathbf{x}_m) \right) \]  

(A.38)

Here, the set of indices of the instances having \( 0 < a_n < C \) is denoted by \( \mathcal{M} \).
A.4 Constructing New Kernels

One way in which new valid kernels can be constructed, is to use simpler kernels as building blocks to build them. Given the kernels $k_1(x, x')$ and $k_2(x, x')$, the properties listed in Eq. A.39–A.48 can be used to construct new kernels.

\[
\begin{align*}
k(x, x') &= ck_1(x, x') \quad \text{(A.39)} \\
k(x, x') &= f(x)k_1(x, x')f(x') \quad \text{(A.40)} \\
k(x, x') &= q(k_1(x, x')) \quad \text{(A.41)} \\
k(x, x') &= \exp(k_1(x, x')) \quad \text{(A.42)} \\
k(x, x') &= k_1(x, x') + k_2(x, x') \quad \text{(A.43)} \\
k(x, x') &= k_1(x, x')k_2(x, x') \quad \text{(A.44)} \\
k(x, x') &= k_3(\phi(x), \phi(x')) \quad \text{(A.45)} \\
k(x, x') &= x^T A x' \quad \text{(A.46)} \\
k(x, x') &= k_a(x_a, x'_a) + k_b(x_b, x'_b) \quad \text{(A.47)} \\
k(x, x') &= k_a(x_a, x'_a)k_b(x_b, x'_b) \quad \text{(A.48)}
\end{align*}
\]

Here, $x$ is an input vector, $c > 0$ is a constant, $f(\cdot)$ denotes any function, $q(\cdot)$ denotes a polynomial having nonnegative coefficients and $\phi(x)$ is a transformation from $x$ to $\mathbb{R}^M$. The function $k_3(\cdot, \cdot)$ is a valid kernel in $\mathbb{R}^M$, $A$ is a positive semidefinite symmetric matrix, $x_a$ and $x_b$ are variables with $x = (x_a, x_b)$, and $k_a$ and $k_b$ are valid kernels, each over their own respective spaces.

A.5 Karush-Kuhn-Tucker Conditions

Karush-Kuhn-Tucker (KKT) conditions arise when a function $f(x)$ has to be maximised while taking a constraint $g(x) \geq 0$ into account. A solution is found by optimising the Lagrangian function

\[
L(x, \lambda) = f(x) + \lambda g(x)
\]  

(A.49)

where $\lambda$ is a Lagrange multiplier, with respect to $\lambda$ and $x$, subjected to the following constraints or conditions:
\[ g(x) \geq 0 \quad (A.50) \]
\[ \lambda \geq 0 \quad (A.51) \]
\[ \lambda g(x) = 0 \quad (A.52) \]
Appendix B

Artificial Neural Network Training

Introduction

This appendix contains additional information and derivations related to the training of artificial neural networks, discussed in section 2.2.4.4. The main source was [92].

B.1 Network Training

A simple method for determining the parameters \( w \) of the simple feed-forward neural network is by minimising the error function

\[
E(w) = \frac{1}{2} \sum_{n=1}^{N} \| y(x_n, w) - t_n \|^2
\]  

(B.1)

where \( \{x_n\} \), with \( n = 1, \ldots, N \) is the set of input training feature vectors and where the set \( \{t_n\} \) consists of the corresponding target values. A more general outlook on network training, however, can be provided by first interpreting network outputs in a probabilistic manner, in the process motivating the choice of activation function used for the output layer as well as the choice of the specific error function to minimise.

The problem we consider here is one in which an input instance must be classified as being one of \( K \) distinct classes. The target values \( t_k \in \{0, 1\} \) are encoded with a 1-of-\( K \) scheme in order to indicate the class - to illustrate this, see Eq. B.2 below for the case where \( K = 3 \). Three objects \( (o_1, o_2 \text{ and } o_3) \) are shown: they belong to classes 1 (left), 2 (middle) and 3 (right).
Appendix B. Artificial Neural Network Training

\[
o_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad o_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad o_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.
\] (B.2)

Network outputs are probabilistically interpreted as being

\[
y_k(x, w) = P(t_k = 1|x).
\] (B.3)

This is done through the application of the softmax function\(^1\) to the output activations \(a_k\), as is shown here:

\[
y_k(x, w) = \frac{\exp(a_k(x, w))}{\sum_j \exp(a_j(x, w))}
\] (B.5)

with \(j = 1, \ldots, K\), where \(0 \leq y_k \leq 1\) and \(\sum_k y_k = 1\). The error function, given by the negative of the log likelihood, is the cross-entropy of the output and target values, and is as follows:

\[
E(w) = -\sum_{n=1}^{N} \sum_{k=1}^{K} t_{kn} \ln y_k(x_n, w)
\] (B.6)

This is then the error function that has to be minimised in order to determine \(w\). \(E(w)\), being a smooth and continuous function, will have its minimum value at some point in the weight space where its gradient is equal to zero, such that

\[
\nabla E(w) = 0
\] (B.7)

and the goal here is to determine a vector \(w\) in order for the above to be true. Because \(E(w)\) has a nonlinear dependence on the \(w\) parameters, many solutions in weight space will correspond with the gradient vanishing - finding the global minimum may not be needed for the successful

\(^1\)In probability theory, the softmax function is applied to a \(K\)-dimensional vector \(s = (s_1, \ldots, s_K)\) of real values to transform it into the vector \(r\) of the same dimension, where each of \(r\)'s real-valued elements now falls in the range (0, 1). The softmax function is as follows:

\[
r_k = \frac{\exp(s_k)}{\sum_j \exp(s_j)}, \quad \text{with } k = 1, \ldots, K \text{ and } j = 1, \ldots, K
\] (B.4)

Since the elements of the new vector \(r\) have values between 0 and 1 and sum to 1, they now form a categorical probability distribution.
implementation of the neural network, but comparing a number of local minima might be required for the finding of an adequately accurate solution.

We employ iterative numerical methods to find a solution to Eq. B.7. Mostly, methods for this task require that some initial vector \( w^{(0)} \) be chosen, and the weight space is then traversed in iterative steps

\[
\mathbf{w}^{(\tau + 1)} = \mathbf{w}^{(\tau)} + \Delta \mathbf{w}^{(\tau)} \tag{B.8}
\]

in order to reach a minimum in the error function, where the gradient will be zero. Here, \( \tau \) denotes the iteration step. We next look at the Taylor expansion of the error function around a point in weight space \( \hat{w} \), as this local quadratic approximation of \( E(\mathbf{w}) \) gives insight into the problem and the methods used for solving it. The approximation is shown in Eq. B.9

\[
E(\mathbf{w}) \simeq E(\hat{\mathbf{w}}) + (\mathbf{w} - \hat{\mathbf{w}})^T \mathbf{b} + \frac{1}{2}(\mathbf{w} - \hat{\mathbf{w}})^T \mathbf{H}(\mathbf{w} - \hat{\mathbf{w}}) \tag{B.9}
\]

where \( \mathbf{b} \) denotes the error function’s gradient at \( \hat{\mathbf{w}} \), as

\[
\mathbf{b} \equiv \nabla E|_{w=\hat{w}} \tag{B.10}
\]

and where \( \mathbf{H} \) is called the Hessian matrix (\( \mathbf{H} = \nabla \nabla E \)) with elements

\[
(H)_{ij} \equiv \frac{\partial E}{\partial \mathbf{w}_i \partial \mathbf{w}_j}|_{\mathbf{w}=\hat{\mathbf{w}}} \tag{B.11}
\]

The local approximation to \( E \)’s gradient, from Eq. B.9, is

\[
\nabla E \simeq \mathbf{b} + \mathbf{H}(\mathbf{w} - \hat{\mathbf{w}}) \tag{B.12}
\]

We use this gradient information to define the weight step update in Eq. B.8 as a step towards the negative gradient of the error function, so that we continuously move closer to a vector \( \mathbf{w} \) where the gradient is zero and we therefore have a minimum of the function. The step update is as follows:

\[
\mathbf{w}^{(\tau + 1)} = \mathbf{w}^{(\tau)} - \eta \nabla E(\mathbf{w}^{(\tau)}) \tag{B.13}
\]
where $\eta > 0$ is called the *learning rate*, and is used to adjust the size of the steps in weight space. Because each step moves the weight vector in the direction that the rate at which the error function decreases is largest, this method is called *gradient descent*. With each new step $\nabla E$ has to be re-evaluated and the whole training set processed to do so. Methods such as this, where the whole training set is used at the same time in order to determine a single step in weight space, are referred to as *batch* methods. Although intuitively pleasing, gradient descent is a rather poor algorithm, and there are faster and more robust batch optimisation methods - *quasi-Newton* methods and *conjugate gradients* being some of them [179–181].

For gradient descent batch methods, one often has to run the algorithm a few times in order to get a solution yielding a sufficient minimum, each run starting with a different random weight vector $w^{(0)}$. This can be a very time-consuming process. Le Cun et al. [182], however, introduced a *Single-step* (or *on-line*) gradient descent version that proved more practical for the purposes of training networks with the use of large training sets. Single-step methods, in contrast to batch methods, make adjustments to the weight vector directly after being presented with a single training instance. Error functions for these methods, founded on maximum likelihood for independent training instances, consist of the summation of the errors for each of the training data instances (where $N$ is the total number of instances), and is expressed as

$$E(w) = \sum_{n=1}^{N} E_n(w)$$  \hspace{1cm} (B.14)

The update rule for on-line gradient descent is then

$$w^{(r+1)} = w^{(r)} - \eta \nabla E_n(w^{(r)})$$  \hspace{1cm} (B.15)

Advantages of single-step gradient descent, as compared to the batch version, is that it can possibly escape local minima and is able to deal with redundancy in the training data set in a more efficient way.

### B.2 Error Backpropagation

This section discusses an efficient method for evaluating $\nabla E$ called *backpropagation*, an approach that involves error-related information being sent forwards and backwards in a neural network. Many learning methods follow an iterative scheme for error function minimisation, with the weight vector being updated after each iterative step, as seen in the previous section. There are two stages involved in each step being taken. During the first stage the error function’s derivatives
Appendix B. Artificial Neural Network Training

must be evaluated with respect to the weight parameters. As backpropagation provides an efficient way of evaluating these derivatives, and seeing that it is during this stage that the backwards propagation of errors takes place, the term “backpropagation” will be used specifically with regard to the evaluation of error function derivatives. The second stage involves the use of the computed derivatives to update the weight vector - the simplest way to do this involves the method of gradient descent and was introduced by Rumelhart et al. [183].

For the derivation of the backpropagation algorithm, we consider a general setup: an arbitrary feed-forward neural network topology, activation functions that are nonlinear and differentiable and a wide range of error functions. Most practical error functions have the form shown in Eq. B.14, given again here as

\[ E(w) = \sum_{n=1}^{N} E_n(w) \]  

We now tackle the problem of determining \( \nabla E_n(w) \). We start with a simple network model where outputs, denoted by \( y_k \), form linear combinations of inputs, denoted by \( x_i \), as

\[ y_k = \sum_i w_{ki} x_i \]  

and where the error function, for the \( n \)th training input instance, looks as follows:

\[ E_n = \frac{1}{2} \sum_k (y_{nk} - t_{nk})^2 \]  

Here, \( y_{nk} = y_k(x_n, w) \). Taking the gradient of \( E_n \) with respect to the weight \( w_{ji} \), we have

\[ \frac{\partial E_n}{\partial w_{ji}} = (y_{nj} - t_{nj}) x_{ni} \]  

which constitutes the product of an error term \( (y_{nj} - t_{nj}) \) corresponding to the output of a connection \( w_{ji} \) and the input of the connection, \( x_{ni} \). We now extend these results to more intricate multilayer feed-forward neural networks where, in the general case, every node determines a linear combination of its input as

\[ a_j = \sum_i w_{ji} z_i \]
with \( z_i \) being either an input or a previous node’s output sending a connection from node \( i \) to node \( j \), and where \( w_{ji} \) is that connection’s corresponding weight. To determine the output \( z_j \) associated with node \( j \), \( a_j \) is transformed using an activation function \( g(\cdot) \), as follows:

\[
z_j = g(a_j) \tag{B.21}
\]

For each training instance, we will suppose that the output of every node in the network has been calculated by using Eq. B.20 and B.21 successively - this is referred to as \textit{forward propagation}, as information flows from the network’s input nodes to its output nodes.

The next step is to evaluate \( E_n \)’s derivative with respect to the weight \( w_{ji} \). Although the outputs of the network’s nodes depend on a specific input instance, we drop the subscript \( n \) to simplify the notation. \( E_n \) depends on \( w_{ji} \) only via \( a_j \), and the partial derivative chain rule can therefore be used to give

\[
\frac{\partial E_n}{\partial w_{ji}} = \frac{\partial E_n}{\partial a_j} \frac{\partial a_j}{\partial w_{ji}} \tag{B.22}
\]

Next, the following notation is introduced:

\[
\delta_j \equiv \frac{\partial E_n}{\partial a_j} \tag{B.23}
\]

Here, \( \delta \) is called an \textit{error}. From Eq. B.20 we see that

\[
\frac{\partial a_j}{\partial w_{ji}} = z_i \tag{B.24}
\]

and by substituting Eq. B.24 and B.23 into Eq. B.22, we arrive at

\[
\frac{\partial E_n}{\partial w_{ji}} = \delta_j z_i \tag{B.25}
\]

From Eq. B.25 it is seen that the derivative of \( E_n \) can be calculated merely by multiplying the \( \delta \)-value for the node at the output side of the link associated with the weight \( w_{ji} \) with the \( z_i \)-value for the node at the input side of the link. This formula then takes a form similar to that determined for the simpler case, given in Eq. B.19. All that is necessary to calculate the derivatives, therefore, is to determine \( \delta_j \) for all hidden and output nodes in the neural network, and to then use Eq. B.25.

For the network’s output nodes, we have
\[ \delta = y_k - t_k \]  

(B.26)

Using the partial derivative chain rule once again, we find \( \delta_j \) for the hidden nodes to be

\[ \delta_j = \frac{\partial E_n}{\partial a_j} = \sum_k \frac{\partial E_n}{\partial a_k} \frac{\partial a_k}{\partial a_j} \]  

(B.27)

where the sum is over all nodes \( k \), where \( k \) labels either hidden or output nodes, receiving a connection from node \( j \). Fig. B.1 shows the configuration of weights, nodes and parameters. Eq. B.27 uses the fact that changes in \( a_j \) causes changes in \( E_n \) through changes in \( a_k \). Substituting Eq. B.23 into Eq. B.27 and using Eq. B.20 and B.21, we arrive at the backpropagation equation given in Eq. B.28, which shows us that in order to determine \( \delta \) for a certain hidden node, the \( \delta \)'s of nodes higher in the network should be propagated backwards.

\[ \delta_j = g'(a_j) \sum_k w_{kj} \delta_k \]  

(B.28)

In the case of batch methods, evaluating the total error’s derivative can be done by carrying out the steps discussed above for each training instance and then summing, as follows:

\[ \frac{\partial E}{\partial w_{ji}} = \sum_n \frac{\partial E_n}{\partial w_{ji}} \]  

(B.29)

**Figure B.1:** Backpropagation.

This illustration helps with the interpretation of Eq. B.28 - where \( \delta_j \) of a hidden node \( j \) is calculated by backpropagating the \( \delta \)-values from the nodes \( k \) receiving connections from \( j \). The top arrow depicts the flow of information during forward propagation, while the two smaller arrows depicts the flow of error information during backpropagation.
Appendix C

Hand-Scanner Classification

This appendix assists in describing the classification system used by the SDSS hand-scanners during visual inspection of images (see section 3.4.1). While Table 3.2 describes each of the different classes and Fig. 3.5 shows a simplified decision tree depicting the classification process followed by the hand-scanners, Table C.1 and C.2 show how the objects in each of these classes look like. Table C.1 shows six $r$-band difference images from each of the ten classes and also illustrate the difference in image-quality based on SNR, while Table C.2 shows difference images of objects from each class in all three bands ($g$, $r$ and $i$).
Table C.1: SDSS hand-scanner classes for different SNR values.

The ten classes, described in Table 3.2, used by the SDSS hand-scanners during visual classification. For each class, six $r$-band images of objects are shown - three of which have an SNR above 40, and three having an SNR below 20 (representing roughly 80% of the dataset).

<table>
<thead>
<tr>
<th>Original Class</th>
<th>Good Quality (SNR &gt; 40)</th>
<th>Bad Quality (SNR &lt; 20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artefact</td>
<td><img src="image" alt="Artefact" /></td>
<td><img src="image" alt="Artefact" /></td>
</tr>
<tr>
<td>Dipole</td>
<td><img src="image" alt="Dipole" /></td>
<td><img src="image" alt="Dipole" /></td>
</tr>
<tr>
<td>Saturated Star</td>
<td><img src="image" alt="Saturated Star" /></td>
<td><img src="image" alt="Saturated Star" /></td>
</tr>
<tr>
<td>Moving</td>
<td><img src="image" alt="Moving" /></td>
<td><img src="image" alt="Moving" /></td>
</tr>
<tr>
<td>Variable</td>
<td><img src="image" alt="Variable" /></td>
<td><img src="image" alt="Variable" /></td>
</tr>
<tr>
<td>Transient</td>
<td><img src="image" alt="Transient" /></td>
<td><img src="image" alt="Transient" /></td>
</tr>
<tr>
<td>SN Other</td>
<td><img src="image" alt="SN Other" /></td>
<td><img src="image" alt="SN Other" /></td>
</tr>
<tr>
<td>SN Bronze</td>
<td><img src="image" alt="SN Bronze" /></td>
<td><img src="image" alt="SN Bronze" /></td>
</tr>
<tr>
<td>SN Silver</td>
<td><img src="image" alt="SN Silver" /></td>
<td><img src="image" alt="SN Silver" /></td>
</tr>
<tr>
<td>SN Gold</td>
<td><img src="image" alt="SN Gold" /></td>
<td><img src="image" alt="SN Gold" /></td>
</tr>
</tbody>
</table>
Table C.2: SDSS hand-scanner classes in different bands.
The ten classes, described in Table 3.2, used by the SDSS hand-scanners during visual classification. For each class, one object is shown in all three bands ($g$, $r$ and $i$).

<table>
<thead>
<tr>
<th>Original Class</th>
<th>$g$-band</th>
<th>$i$-band</th>
<th>$r$-band</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artefact</td>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
</tr>
<tr>
<td>Dipole</td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
<td><img src="image6" alt="Image" /></td>
</tr>
<tr>
<td>Saturated Star</td>
<td><img src="image7" alt="Image" /></td>
<td><img src="image8" alt="Image" /></td>
<td><img src="image9" alt="Image" /></td>
</tr>
<tr>
<td>Moving</td>
<td><img src="image10" alt="Image" /></td>
<td><img src="image11" alt="Image" /></td>
<td><img src="image12" alt="Image" /></td>
</tr>
<tr>
<td>Variable</td>
<td><img src="image13" alt="Image" /></td>
<td><img src="image14" alt="Image" /></td>
<td><img src="image15" alt="Image" /></td>
</tr>
<tr>
<td>Transient</td>
<td><img src="image16" alt="Image" /></td>
<td><img src="image17" alt="Image" /></td>
<td><img src="image18" alt="Image" /></td>
</tr>
<tr>
<td>SN Other</td>
<td><img src="image19" alt="Image" /></td>
<td><img src="image20" alt="Image" /></td>
<td><img src="image21" alt="Image" /></td>
</tr>
<tr>
<td>SN Bronze</td>
<td><img src="image22" alt="Image" /></td>
<td><img src="image23" alt="Image" /></td>
<td><img src="image24" alt="Image" /></td>
</tr>
<tr>
<td>SN Silver</td>
<td><img src="image25" alt="Image" /></td>
<td><img src="image26" alt="Image" /></td>
<td><img src="image27" alt="Image" /></td>
</tr>
<tr>
<td>SN Gold</td>
<td><img src="image28" alt="Image" /></td>
<td><img src="image29" alt="Image" /></td>
<td><img src="image30" alt="Image" /></td>
</tr>
</tbody>
</table>
Appendix D

Implementation of Naïve Bayes

This appendix shows the MATLAB® implementation of our Naïve Bayes (NB) algorithm. It shows six functions: Main.m (section D.1), the main program from which all the functions necessary for the training and testing of NB are called; BAYES_INPUT.m (section D.2), generating the required inputs for the training of NB; BINS.m (section D.3), responsible for the binning calculations of the algorithm; TRAIN_BAYES.m (section D.4), the function used to train NB; TEST_BAYES.m (section D.5), the function used for testing and RESULTS.m (section D.6), responsible for calculating the performance metrics. All of these functions are further described in their respective comments sections.

D.1 The Main Program

%Author: Lise du Buisson
%This is the main program from which NB will be run.
%The original input .txt files whose filenames are specified below (look at
%input_train, input_test and input_other) details one object instance per row
%and have the following comma-separated columns:
% - ID is the object's identification number
% - f1, ..., fn are the different feature values
% - c1 is a class system used by a collaborator - the details are unimportant here
% - c2 is the true class values ("1", "2" or "3") to distinguish between our
% three visual classes
% - c3 is true main class values ("0" or "1") to distinguish between not-real
% and real objects (this will be used for training and testing)
%---------------------------------------------------------------------
%counters
numberPCA = [50];
LDAf = 'False';
LDAt = 'True';
normf = 'False';
normt = 'True';
counter = 1;

%read, train and test all the different feature sets
for pca = 1:length(numberPCA)
    for lda = 1:1
        LDA = LDAf;
        else
            LDA = LDAt;
        end
        for nrm = 1:1
            NORM = normf;
            else
                NORM = normt;
        end
        %display counter:
        SETNAME = strcat(num2str(counter), '__PCA',
            num2str(numberPCA(pca)), '__LDA', LDA, '__norm', NORM);
        disp(SETNAME);
        %construct filenames:
        %input training, validation and testing set:
        input train = strcat('features75percent\TRAINING\imageSize31\PCA',
            num2str(numberPCA(pca)), '__LDA', LDA, '__FeatureNormalize',
            NORM, '_features.txt');
        input test = strcat('features25percent\TEST\imageSize31\PCA',
            num2str(numberPCA(pca)), '__LDA', LDA, '__FeatureNormalize',
            NORM, '_features.txt');
        input other = strcat('features75percent\TEST\imageSize31\PCA',
            num2str(numberPCA(pca)), '__LDA', LDA, '__FeatureNormalize',
            NORM, '_features.txt');
        %classified input training, validation and testing sets above:
        input_train_classified = strcat('features25percent\classified\'
            TRAINING\imageSize31\PCA', num2str(numberPCA(pca)), '__LDA', LDA,
            '__FeatureNormalize', NORM, '_features_classified.txt');
        input_test_classified = strcat('features25percent\classified\'
            TEST\imageSize31\PCA', num2str(numberPCA(pca)), '__LDA', LDA,
            '__FeatureNormalize', NORM, '_features_classified.txt');
        input_other_classified = strcat('features75percent\classified\'
            TEST\imageSize31\PCA', num2str(numberPCA(pca)), '__LDA', LDA,
D.2 Algorithm Input

```matlab
function [X_test, Y_test, X_train, Y_train, bins, bin_vec] = BAYES_INPUT(input_test, input_train, input_other)

%This program generates the required inputs for new_TRAIN_BAYES().

% X_train: matrix; each row consists of the features of one object in the
% training set.
% Y_train: vector; each row contains the known class of the instance in the
% corresponding rows in X_train.
% X_test: matrix; each row consists of the features of one object in the
```
% test/validation set.
% Y_test: vector; each row contains the known class of the instance in the corresponding rows in X_test.
%----------------------------------------------------------------------------------------
%----------------------------------------------------------------------------------------
%----------------------------------------------------------------------------------------
% Read files into matrices
%test = csvread(input_test, 0, 0);  
%train = csvread(input_train, 0, 0);  
%other = csvread(input_other, 0, 0);  
%stest = size(test);  

X_test = test(:, 2:stest(2)-3);  
Y_test = test(:, stest(2));  
X_train = train(:, 2:stest(2)-3);  
Y_train = train(:, stest(2));  
X_other = other(:, 2:stest(2)-3);  

%calculate bins
[bins, bin_vec] = BINS(X_train, X_test, X_other);  
fclose('all');

D.3 Calculating the Bins

function [bins, bin_vec] = BINS(X_train, X_test, X_other)  
%This program calculates the number of bins and the bin separation values
%(edge-values) for each feature.
%----------------------------------------------------------------------------------------
%----------------------------------------------------------------------------------------
%sz = size(X_train);  
%amount_of_features = sz(2);  
data_points = sz(1);  

%create a matrix (bin_vec) to store the amount of bins required for each feature in the dataset, as well as each feature's maximum and minimum
%value (across the whole dataset).
%rows = different features
%col1 = number of bins for feature
%col2 = feature maximum value
%col3 = feature minimum value
bin_vec = zeros(amount_of_features, 3);

%fill bin_vec with values:
for u = 1:amount_of_features
    %calculate the number of bins (same for every feature):
    numberOfBins = data_points / 2;
    numberOfBins = numberOfBins / 4; %average of roughly 4 objects per bin.
    numberOfBins = round(numberOfBins);
    %get the maximum and minimum values of this feature in the
    %training, validation and test set.
    maxf = zeros(3,1);
    minf = zeros(3,1);
    maxf(1,1) = max(max(X_train(:,u)));
    maxf(2,1) = max(max(X_test(:,u)));
    maxf(3,1) = max(max(X_other(:,u)));
    minf(1,1) = min(min(X_train(:,u)));
    minf(2,1) = min(min(X_test(:,u)));
    minf(3,1) = min(min(X_other(:,u)));
    %the absolute maximum and minimum for this feature for the
    %whole dataset is then:
    maxi = max(max(maxf(:,1)));
    mini = min(min(minf(:,1)));
    %store the number of bins, the maximum and the minimum:
    bin_vec(u,1) = numberOfBins;
    bin_vec(u,2) = maxi;
    bin_vec(u,3) = mini;
end

%determine the maximum amount of bins used for any feature (although this seems
%redundant in the case here where all features have an equal number of bins,
%this code makes allowance for the case where different features have
%different numbers of bins.)
max_bins = max(max(bin_vec(:,1)));
max_bins = max_bins(1);
%a = number of bin edges
a = max_bins + 1;

%create the empty "bins" matrix: the edge-values of the bins for each feature will
%be stored in it.
bins = zeros(amount_of_features, a);
sib = size(bins);

%store the edge-values in "bins" for each feature
for y = 1:amount_of_features
    %get the maximum and minimum value of the feature
    maxi = bin_vec(y,2);
    mini = bin_vec(y,3);

    %determine step size
    step = (maxi-mini)/bin_vec(y,1);

    %do the edges
    bins(y,1) = mini;
    val = mini;
    for t = 2:(bin_vec(y,1)+1)
        if t == bin_vec(y,1)+1
            val = val + step;
            bins(y,t) = val;
        else
            val = maxi + 0.000000000001;
        end
        bins(y,t) = val;
    end
    sub = sib(2) - (bin_vec(y,1)+1);
    if sub ~= 0
        for e = 1:sub
            bins(y, sib(2)-sub+e) = val;
        end
    end
end

D.4 Training Naïve Bayes

function [prob, frac_0, frac_1] = TRAIN_BAYES(X_train, Y_train, bins, bin_vec)

%The goal of this program is to create a 3D matrix containing the conditional
%probabilities (obtained from frequency counts using the training data) of objects
%(given their class) having certain feature values.

%prob: matrix; used for storing the conditional probabilities mentioned above.
%frac_0: prior probability of class "0".
%frac_1: prior probability of class "1".
%-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
%determine the number of different classes (2 in our case: "1" and "0")
Y_u = unique(Y_train);
number_of_classes = length(Y_u);

%create empty "countj" 3D matrix for storing frequency counts
countj = zeros(s(2),a(2)-1,number_of_classes);

%create fraction variables (prior probabilities for class "0" and class "1")
frac_0 = 0;
frac_1 = 0;

%obtain the "countj" matrix
for i=1:number_of_classes
    indi = find(Y_train == Y_u(i));
    datai = X_train(indi,:);
    sdatai = size(datai);
    if Y_u(i) == 0
        frac_0 = sdatai(1)/total;
    elseif Y_u(i) == 1
        frac_1 = sdatai(1)/total;
    end
    for j = 1:s(2) %loop through all the features
        validEdges = bin_vec(j,1)+1;
        featurejBinned = histc(datai(:,j), bins(j,1:validEdges));
        featurejBinned = featurejBinned(1:bin_vec(j,1));
        rest = a(2)-1-bin_vec(j,1);
        if rest ~= 0
            for zer = (bin_vec(j,1)+1):(a(2)-1)
                featurejBinned(zer) = 0.0;
            end
        end
        countj(j,:,i) = featurejBinned; %vector of counts for feature j
    end
end

%create the probability matrix
prob = zeros(s(2),a(2)-1,number_of_classes);
Appendix D. Implementation of Naïve Bayes

59 $\text{obtain the probability matrix}$
60 $\text{sc} = \text{size(countj);}$
61 $\text{for } i = 1:sc(1) $\text{ loop through all the features}$
62 $\text{validBinsForThisFeature = binvec}(i,1);$
63 $\text{for } j = 1:validBinsForThisFeature $\text{ loop through the valid bins}$
64 $\text{for } k = 1:sc(3) $\text{ loop through all the classes}$
65 $\% \text{includes the use of Laplace smoothing:}$
66 $\text{prob}(i,j,k) = (1 + \text{countj}(i,j,k))/(\text{binvec}(i,1) + \text{sum}(\text{countj}(i,:,k)));$
67 $\text{end}$
68 $\text{end}$
69 $\text{end}$

D.5 Testing Naïve Bayes

1 function $[\text{C\_test}] = \text{TEST\_BAYES}(X\_test, Y\_test, X\_train, Y\_train, bins, prob,$
2 $\text{frac\_0, frac\_1, select\_test, select\_train, output, threshold, thresholdValue,$
3 $\text{input\_test, input\_test\_classified, input\_train, input\_train\_classified})$
4
5 $\% \text{The purpose of this function is to assign a class to each of the objects}$
6 $\% \text{in the rows of both } X\_test \text{ and } X\_train. \text{ This will then be used to output}$
7 $\% \text{classified.txt files, from where RESULTS.m can be used to calculate the}$
8 $\% \text{performance metrics.}$
9 $
10 \% \text{C\_test: vector; each row contains the predicted class of the corresponding test}$
11 $\% \text{object in } X\_test.$
12 $\% \text{If select\_test == 1, classify the test set, otherwise don't.}$
13 $\% \text{If select\_train == 1, classify the training set, otherwise don't.}$
14 $\% \text{If output == 1, create the 'classified.txt' files, otherwise don't.}$
15 $\% \text{If threshold == 1, take the prior probabilities of the classes into account, else}$
16 $\% \text{don't. (This is not valid anymore - ensure that it is always 0).}$
17 $\% \text{Set thresholdValue to 0 for standard NB where an object belongs to the class}$
18 $\% \text{resulting in the highest probability } P(\text{Class|object\_features}).$
19 $\% \text{-----------------------------------------------------------------}$
20 $\% \text{-----------------------------------------------------------------}$
21 $\% \text{classify test set.}$
22 $\% \text{- - - - - - - - - - - - - - - - - -}$
23 $\text{if select\_test == 1}$
24 $\quad \text{stest = size}(X\_test);$  
25 $\quad \text{sb = size}(bins);$  
26 $\quad \text{C\_test} = \text{zeros}(\text{stest}(1), 1);$  
27 $\text{end}$
28
29
%determine the number of different classes
Y_test_small = unique(Y_test);  % 0, 1
number_of_classes = length(Y_test_small);

%classify the data points
for i = 1:stest(1)  %loop through data points
    class_vector_test = zeros(number_of_classes, 1);
    for j = 1:stest(2)  %loop through classes
        class_prob = 1.0;
        for k = 1:stest(2)  %loop through features
            %determine the bin's probability index that you need
            feature_value = X_test(i,k);
            gotprob = 0;
            for t = 1:stest(2)-1  %loop through the bins
                if (feature_value >= bins(k,t)) && (feature_value < bins(k,t+1))
                    class_prob = class_prob * prob(k,t,j);
                    gotprob = 1;
                    break;
                end
            end
        end
        %find the right class fraction (prior probability) to multiply with.
        if Y_test_small(j) == 0
            class_prob = class_prob * frac0;
        elseif Y_test_small(j) == 1
            class_prob = class_prob * frac1;
        end
        class_vector_test(j, 1) = class_prob;
    end
    %working with the object and its probabilities now:
    if threshold == 0
        maxclass = find(class_vector_test == max(max(class_vector_test)));
        if length(maxclass) > 1
            maxclass = maxclass(2);
        end
        C_test(i, 1) = maxclass - 1;
        Pred_Prob(i,1) = (class_vector_test(2,1) / (class_vector_test(2,1) + class_vector_test(1,1)));
    else
        class_0_prob = class_vector_test(1,1);
        class_1_prob = class_vector_test(2,1);
        ratio = class_1_prob / class_0_prob;
        if ratio >= thresholdValue
            %then real wins
            C_test(i,1) = 1;
        else
            C_test(i,1) = 1;
        end
    end
else
  \%then not-real wins
  C_test(i,1) = 0;
end
end
C_test = C_test(1,:);

class_training = [class_training C_test];

class_training(1,:) = size(X_train);
sb = size(bins);
C_train = zeros(class_training(1,:), 1);

\%determine the number of different classes
Y_train_small = unique(Y_train);  \% 0, 1
number_of_classes = length(Y_train_small);

\%classify the data points
for i = 1:class_training(1,:)
  %loop through data points
  class_vector_train = zeros(number_of_classes, 1);
  for j = 1:number_of_classes  \%loop through classes
    class_prob = 1;
    for k = 1:class_training(2,:)
      %loop through features
      \%determine the bin's probability index that you need
      feature_value = X_train(i,k);
gotprob = 0;
      for t = 1:sb(2)-1  \%loop through the bins
        if (feature_value >= bins(k,t)) \&\& (feature_value < bins(k, t+1))
          class_prob = class_prob * prob(k, t, j);
gotprob = 1;
        break;
      end
  end
  \%
  \%find the right class fraction to multiply with.
  if Y_train_small(j) == 0
    class_prob = class_prob * frac_0;
  elseif Y_train_small(j) == 1
    class_prob = class_prob * frac_1;
  end
  class_vector_train(j, 1) = class_prob;
end

if select_train == 1
  strain = size(X_train);
sb = size(bins);
C_train = zeros(strain(1), 1);

\%determine the number of different classes
Y_train_small = unique(Y_train);  \% 0, 1
number_of_classes = length(Y_train_small);

\%classify the data points
for i = 1:strain(1)
  %loop through data points
  class_vector_train = zeros(number_of_classes, 1);
  for j = 1:number_of_classes  \%loop through classes
    class_prob = 1;
    for k = 1:strain(2)
      %loop through features
      \%determine the bin's probability index that you need
      feature_value = X_train(i,k);
gotprob = 0;
      for t = 1:sb(2)-1  \%loop through the bins
        if (feature_value >= bins(k,t)) \&\& (feature_value < bins(k, t+1))
          class_prob = class_prob * prob(k, t, j);
gotprob = 1;
        break;
      end
  end
  \%
  \%find the right class fraction to multiply with.
  if Y_train_small(j) == 0
    class_prob = class_prob * frac_0;
  elseif Y_train_small(j) == 1
    class_prob = class_prob * frac_1;
  end
  class_vector_train(j, 1) = class_prob;
end
if threshold == 0
    maxclass = find(class_vector_train == max(max(class_vector_train)));  
    maxclass = maxclass(1);  
    C_train(i, 1) = maxclass - 1;  
else
    class_0_prob = class_vector_train(1,1);  
    class_1_prob = class_vector_train(2,1);  
    ratio = class_1_prob / class_0_prob;  
    if ratio >= thresholdValue  
        %then real wins  
        C_train(i,1) = 1;  
    else  
        %then not-real wins  
        C_train(i,1) = 0;  
    end  
end  
end

%now make the _classified.txt outputs.  
%---------------------------------------  
%---------------------------------------  
if output == 1  
%test-case:  
%-----------  
if select_test == 1
    test_mat = csvread(input_test, 0, 0);  
    sz = size(test_mat);  
    test_out = fopen(input_test_classified, 'wb', 'b', 'UTF-8');  
    test_classified = zeros(sz(1), sz(2)+1);  
    test_classified(:, 1:sz(2)) = test_mat;  
    test_classified(:, sz(2)+1) = C_test;  
    sc = size(test_classified);  
    %print the file  
    for i = 1:sc(1)  
        for j = 1:sc(2)
If $j = 1$

```c
s = sprintf('%i', test_classified(i, j));
```

If length(s) == 9

```c
res = 9 - length(s);
while res > 0
    s = strcat('0', s);
    res = res - 1;
end
```

If $i = 1$

```c
fprintf(test_out, '%s', s);
else
    fprintf(test_out, '
%s', s);
end
```

Elseif $(j == sc(2)) || (j == sc(2)-1) || (j == sc(2)-2) || (j == sc(2)-3)$

```c
fprintf(test_out, ', %i', test_classified(i, j));
```

Else

```c
fprintf(test_out, ', %.5E', test_classified(i, j));
```

End

End

Fclose(test_out);

%training-case:

%----------------

If select_train == 1

```c
train_mat = csvread(input_train, 0, 0);
bla = size(train_mat);
```

```c
train_out = fopen(input_train_classified, 'wb', 'b', 'UTF-8');
```

```c
train_classified = zeros(bla(1), bla(2)+1);
```

```c
train_classified(:, 1:bla(2)) = train_mat;
```

```c
train_classified(:, bla(2)+1) = C_train;
```

```c
sa = size(train_classified);
```

%print the file

```c
for i = 1:sa(1)
    for j = 1:sa(2)
        if j == 1
            s = sprintf('%i', train_classified(i, j));
```

if length(s) == 9
    res = 9 - length(s);
    while res > 0
        s = strcat('0', s);
        res = res - 1;
    end
end

if i == 1
    fprintf(train_out, '%s', s);
else
    fprintf(train_out, '\n%s', s);
end
elseif (j == sa(2)) || (j == sa(2)-1) || (j == sa(2)-2) || (j == sa(2)-3)
    fprintf(train_out, ', %i', train_classified(i,j));
else
    fprintf(train_out, ', %.5E', train_classified(i,j));
end
end
end
fclose(train_out);
end
fclose('all');

D.6 Calculating Performance Metrics

function [acc] = RESULTS(test_results, test_classified)
%This function reads in a text-file with the classified data and determines
%the performance metrics based on that. It also writes the results in an
%output file.
%------------------------------------------------------------------------
%------------------------------------------------------------------------
%create the output file for the results.
results_out = fopen(test_results, 'wb', 'b', 'UTF-8');
%load the classified data text file into a matrix.
classified_data = csvread(test_classified, 0, 0);
%get the known and predicted classification.
sd = size(classified_data);
known = classified_data(:,sd(2)-1);
classified = classified_data(:, sd(2));
%determine the confusion-matrix and calculate the performance metrics.
[mat, order] = confusionmat(known, classified);
acc = ((mat(1,1) + mat(2,2)) / (mat(1,1) + mat(1,2) + mat(2,1) + mat(2,2)));
pre = mat(2,2) / (mat(2,2) + mat(1,2));
rec = mat(2,2) / (mat(2,2) + mat(2,1));
f1 = (2 * rec * pre) / (rec + pre);
%print the output file.
fprintf(results_out, 'acc, pre, rec, f1, mat(1,1), mat(1,2), mat(2,1), mat(2,2),
order(1), order(2)');
fprintf(results_out, 'n%.2f, %.2f, %.2f, %.2f, %d, %d, %d, %d, %i, %i', acc, pre, rec, f1, mat(1,1), mat(1,2), mat(2,1), mat(2,2), order(1), order(2));
fclose('all'); end
Bibliography


