Deep Learning for Natural Language Processing: A Gentle Introduction

Mihai Surdeanu and Marco A. Valenzuela-Escárcega
Department of Computer Science
University of Arizona

March 25, 2021

Contents

Preface

An obvious question that may pop up when seeing this material is: ”Why another deep learning and natural language processing book?” Several excellent ones have been published, covering both theoretical and practical aspects of deep learning and its application to language processing. However, from my experience teaching courses on natural language processing, I argue that, despite their excellent quality, most of these books do not target their most likely readers. The intended reader of this book is one who is skilled in a domain other than machine learning and natural language processing and whose work relies, at least partially, on the automated analysis of large amounts of data, especially textual data. Such experts may include social scientists, political scientists, biomedical scientists, and even computer scientists and computational linguists with limited exposure to machine learning.

Existing deep learning and natural language processing books generally fall into two camps. The first camp focuses on the theoretical foundations of deep learning. This is certainly useful to the aforementioned readers, as one should understand the theoretical aspects of a tool before using it. However, these books tend to assume the typical background of a machine learning researcher and, as a consequence, I have often seen students who do not have this background rapidly get lost in such material. To mitigate this issue, the second type of book that exists today focuses on the machine learning practitioner; that is, on how to use deep learning software, with minimal attention paid to the theoretical aspects. I argue that focusing on practical aspects is similarly necessary but not sufficient. Considering that deep learning frameworks and libraries have gotten fairly complex, the chance of misusing them due to theoretical misunderstandings is high. I have commonly seen this problem in my courses, too.

This book, therefor, aims to bridge the theoretical and practical aspects of deep learning for natural language processing. I cover the necessary theoretical background and assume minimal machine learning background from the reader. My aim is that anyone who took linear algebra and calculus courses will be able to follow the theoretical material. To address practical aspects, this book includes pseudo code for the simpler algorithms discussed and actual Python code for the more complicated architectures. The code should be understandable by anyone who has taken a Python programming course. After reading this book, I expect that the reader will have the necessary foundation to immediately begin building real-world, practical natural language processing systems, and to expand their knowledge by reading research publications on these topics.

Acknowledgments

Your acknowledgments: TODO: Thank you to all the people who helped!

Mihai and Marco

1 Introduction

Machine learning (ML) has become a pervasive part of our lives. For example, Pedro Domingos, a machine learning faculty member at University of Washington, discusses a typical day in the life of a 21st century person, showing how she is accompanied by machine learning applications throughout the day from early in the morning (e.g., waking up to music that the machine matched to her preferences) to late at night (e.g., taking a drug designed by a biomedical researcher with the help of a robot scientist) [**?**].

Natural language processing (NLP) is an important subfield of ML. As an example of its usefulness, consider that PubMed, a repository of biomedical publications built by the National Institutes of Health,[1] has indexed more than one million research publications *per year* since 2010 [**?**]. Clearly, no human reader (or team of readers) can process so much material. We need machines to help us manage this vast amount of knowledge. As one example out of many, an inter-disciplinary collaboration that included our research team showed that machine reading discovers an order of magnitude more protein signaling pathways[2] in biomedical literature than exist today in humanly-curated knowledge bases [**?**]. Only 60 to 80% of these automatically-discovered biomedical interactions are correct (a good motivation for *not* letting the machines work alone!). But, without NLP, all of these would remain "undiscovered public knowledge" [**?**], limiting our ability to understand important diseases such as cancer. Other important and more common applications of NLP include web search, machine translation, and speech recognition, all of which have had a major impact in almost everyone's life.

Since approximately 2014, the "deep learning tsunami" has hit the field of NLP [**?**] to the point that, today, a majority of NLP publications use deep learning. For example, the percentage of deep learning publications at four top NLP conferences has increased from under 40% in 2012 to 70% in 2017 [**?**]. There is good reason for this domination: deep learning systems are relatively easy to build (due to their modularity), and they perform better than many other ML methods.[3] For example, the site nlpprogress.com, which keeps track of state-of-the-art results in many NLP tasks, is dominated by results of deep learning approaches.

[1] https://www.ncbi.nlm.nih.gov/pubmed/

[2] Protein signaling pathways "govern basic activities of cells and coordinate multiple-cell actions". Errors in these pathways "may cause diseases such as cancer". See: https://en.wikipedia.org/wiki/Cell_signaling

[3] However, they are not perfect. See Section 1.3 for a discussion.

This book explains deep learning methods for NLP, aiming to cover both theoretical aspects (e.g., how do neural networks learn?) and practical ones (e.g., how do I build one for language applications?).

The goal of the book is to do this while assuming minimal technical background from the reader. The theoretical material in the book should be completely accessible to the reader who took linear algebra, calculus, and introduction to probability theory courses, or who is willing to do some independent work to catch up. From linear algebra, the most complicated notion used is matrix multiplication. From calculus, we use differentiation and partial differentiation. From probability theory, we use conditional probabilities and independent events. The code examples should be understandable to the reader who took a Python programming course.

Starting nearly from scratch aims to address the background of what we think will be the typical reader of this book: an expert in a discipline other than ML and NLP, but who needs ML and NLP for her job. There are many examples of such disciplines: the social scientist who needs to mine social media data, the political scientist who needs to process transcripts of political discourse, the business analyst who has to parse company financial reports at scale, the biomedical researcher who needs to extract cell signaling mechanisms from publications, etc. Further, we hope this book will also be useful to computer scientists and computational linguists who need to catch up with the deep learning wave. In general, this book aims to mitigate the impostor syndrome [**?**] that affects many of us in this era of rapid change in the field of machine learning and artificial intelligence (this author certainly has suffered and still suffers from it![4]).

1.1 What this Book Covers

This book interleaves chapters that discuss the theoretical aspects of deep learning for NLP with chapters that focus on implementing the previously discussed theory. For the implementation chapters we will use PyTorch, a deep learning library that is well suited for NLP applications.[5]

Chapter 2 begins the theory thread of the book by attempting to convince the reader that machine learning is easy. We will use a children's book to introduce key ML concepts, including our first learning algorithm. From this example, we will start building several basic neural networks. In the same chapter, we will formalize the Perceptron algorithm, the simplest neural network. In Chapter 3, we will transform the Perceptron into a logistic regression network, another simple neural network that is surprisingly effective for NLP. In Chapters 5 and 6 we will generalize these algorithms into feed forward neural networks, which operate over arbitrary combinations of artificial neurons.

[4] Even the best of us suffer from it. Please see Kevin Knight's description of his personal experience involving tears (not of joy) in the introduction of this tutorial [**?**].

[5] https://pytorch.org

The astute historian of deep learning will have observed that deep learning had an impact earlier on image processing than on NLP. For example, in 2012, researchers at University of Toronto reported a massive improvement in image classification when using deep learning [**?**]. However, it took more than two years to observe similar performance improvements in NLP. One explanation for this delay is that image processing starts from very low-level units of information (i.e., the pixels in the image), which are then hierarchically assembled into blocks that are more and more semantically meaningful (e.g., lines and circles, then eyes and ears, in the case of facial recognition). In contrast, NLP starts from words, which are packed with a lot more semantic information than pixels and, because of that, are harder to learn from. For example, the word *house* packs a lot of common-sense knowledge (e.g., houses generally have windows and doors and they provide shelter). Although this information is shared with other words (e.g., *building*), a learning algorithm that has seen *house* in its training data will not know how to handle the word *building* in a new text to which it is exposed after training.

Chapter 8 addresses this limitation. In it, we discuss word2vec, a method that transforms words into a numerical representation that captures (some) semantic knowledge. This technique is based on an observation that "you shall know a word by the company it keeps" [**?**]; that is, it learns from the context in which words appear in large collections of texts. Under this representation, similar words such as *house* and *building* will have similar representations, which will improve the learning capability of our neural networks. An important limitation of word2vec is that it conflates all senses of a given word into a single numerical representation. That is, the word *bank* gets a single numerical representation regardless of whether its current context indicates a financial sense, e.g., *Bank of America*, or a geological one, e.g., *bank of the river*. In Chapter 10 we will introduce contextualized embeddings, i.e., numerical representations that are sensitive of the current context in which a word appears, which address this limitation. These contextualized embeddings are built using transformer networks, which rely on "attention," a is a mechanism that computes the representation of a word using a weighted average of the representations of the words in its context. These weights are learned and indicate how much "attention" each word should put on each of its neighbors (hence the name).

Chapter 12 introduces sequence models for processing text. For example, while the word *book* is syntactically ambiguous (i.e., it can be either a noun or a verb), knowing that it is preceded by the determiner *the* in a text gives strong hints that this instance of it is a noun. In this chapter, we will cover neural network architectures designed to model such sequences, including recurrent neural networks, convolutional neural networks, long short-term memory networks, and long short-term memory networks combined with conditional random fields.

Chapter 14 discusses sequence-to-sequence methods (i.e., methods tailored for NLP tasks where the input is a sequence and the output is another sequence). The most common example of such a task is machine translation; where the input is a sequence of words in one language, and the output is a sequence that captures the translation of the original text in a new language.

Chapter 15 discusses methods that begin to address the "brittleness" of deep learning when transferring a model from one domain to another. For example, the performance of a part-of-speech tagging system (i.e., identifying which words are nouns, verbs, etc.) that is trained on well-formed texts, such as newspaper articles, drops precipitously when used on social media texts (see Section 1.3 for a longer discussion).

Lastly, Chapter 16 discusses approaches for training neural networks with minimal supervision. For example, training a neural network to detect spam emails normally requires many examples of emails that are/are not spam. In this chapter, we introduce a few recent directions in deep learning that allow the training of a network from a few examples that are annotated with the desired outcome (e.g., spam or not spam) and with many others that are not.

As previously mentioned, the theoretical discussion in these chapters is interleaved with chapters that discuss how to implement these notions in PyTorch. Chapter 4 shows an implementation of the logistic regression algorithm introduced in Chapter 3. Chapter 7 introduces an implementation of the feed forward neural network introduced in Chapters 5 and 6. Chapter 9 enhances the previous implementation of a neural network with the continuous word representations introduced in Chapter 8. Chapter 11 changes the previous implementation of feed forward neural networks to use the contextualized embeddings generated by a transformer network. Lastly, Chapter 13 implements the sequence models introduced in Chapter 12.

1.2 What this Book Does Not Cover

It is important to note that deep learning is only one of the many subfields of machine learning. In his book, Domingos provides an intuitive organization of these subfields into five "tribes" [**?**]:

Connectionists This tribe focuses on machine learning methods that (shallowly) mimic the structure of the brain. The methods described in this book fall into this tribe.

Evolutionaries The learning algorithms adopted by this group of approaches, also known as genetic algorithms, focus on the "survival of the fittest". That is, these algorithms "mutate" the "DNA" (or parameters) of the models to be learned, and preserve the generations that perform the best.

Symbolists The symbolists rely on inducing logic rules that explain the data in the task at hand. For example, a part-of-speech tagging system in this camp may learn a rule such as `if` previous word is *the*, `then` the part of the speech of the next word is noun.

Bayesians The Bayesians use probabilistic models such as Bayesian networks. All these methods are driven by Bayes' rule, which describes the probability of an event.

Analogizers The analogizers' methods are motivated by the observation that "you are what you resemble". For example, a new email is classified as spam because it uses content similar to other emails previously classified as such.

It is beyond the goal of this book to explain these other tribes in detail. Even from the connectionist tribe, we will focus mainly on methods that are relevant for language processing.[6] For a more general description of machine learning, the interested reader should look to other sources such as Domingos' book, or Hal Daumé III's excellent Course in Machine Learning.[7]

1.3 Deep Learning Is Not Perfect

While deep learning has pushed the performance of many machine learning applications beyond what we thought possible just ten years ago, it is certainly not perfect. Gary Marcus and Ernest Davis provide a thoughtful criticism of deep learning in their book, Rebooting AI [**?**]. Their key arguments are:

Deep learning is opaque While deep learning methods often learn well, it is unclear *what* is learned, i.e., what the connections between the network neurons encode. This is dangerous, as biases and bugs may exist in the models learned, and they may be discovered only too late, when these systems are deployed in important real-world applications such as diagnosing medical patients, or self-driving cars.

Deep learning is brittle It has been repeatedly shown both in the machine learning literature and in actual applications that deep learning systems (and for that matter most other machine learning approaches) have difficulty adapting to new scenarios they have not seen during training. For example, self-driving cars that were trained in regular traffic on US highways or large streets do not know how to react to unexpected scenarios such as a firetruck stopped on a highway.[8]

Deep learning has no common sense An illustrative example for this limitation is that object recognition classifiers based on deep learning tend to confuse objects when they are rotated in three-dimensional space, e.g., an overturned bus in the snow is confused with a snow plow. This happens because deep learning systems lack the common-sense knowledge that some object features are inherent properties of the category itself regardless of the object position, e.g., a school bus in the US usually has a yellow roof, while some features are just contingent associations, e.g., snow tends to be present around snow plows. (Most) humans naturally use common sense, which means that we do generalize better to novel instances, especially when they are outliers.

[6] Most of methods discussed in this book are certainly useful and commonly used outside of NLP as well.
[7] http://ciml.info
[8] https://www.teslarati.com/tesla-model-s-firetruck-crash-details/

All the issues raised by Marcus and Davis are unsolved today. However, we will discuss some directions that begin to address them in this book. For example, in Chapter 14 we will discuss algorithms that (shallowly) learn common-sense knowledge from large collections of texts. In Chapter 15 we will introduce strategies to mitigate the pain in transferring deep learning models from one domain to another.

1.4 Mathematical Notations

While we try to rely on plain language as much as possible in this book, mathematical formalisms cannot (and should not) be avoided. Where mathematical notations are necessary, we rely on the following conventions:

- We use lower case characters such as x to represent scalar values, which will generally have integer or real values.
- We use bold lower case characters such as $\mathbf{x}$ to represent arrays (or vectors) of scalar values, and x_i to indicate the scalar element at position i in this vector. Unless specified otherwise, we consider all vectors to be column vectors during operations such as multiplication, even though we show them in text as horizontal. We use $[\mathbf{x};\mathbf{y}]$ to indicate vector concatenation. For example, if $\mathbf{x} = (1,2)$ and $\mathbf{y} = (3,4)$, then $[\mathbf{x};\mathbf{y}] = (1,2,3,4)$.
- We use bold upper case characters such as $\mathbf{X}$ to indicate matrices of scalar values. Similarly, x_{ij} points to the scalar element in the matrix at row i and column j. $\mathbf{x}_i$ indicates the vector corresponding to the entire row i in matrix $\mathbf{X}$.
- We collectively refer to matrices of arbitrary dimensions as *tensors*. By and large, in this book tensors will have dimension 1 (i.e., vectors) or 2 (matrices). Occasionally, we will run into tensors with 3 dimensions.

2 The Perceptron

This chapter covers the Perceptron, the simplest neural network architecture. In general, neural networks are machine learning architectures loosely inspired by the structure of biological brains. The Perceptron is the simplest example of such architectures: it contains a single artificial neuron.

The Perceptron will form the building block for the more complicated architectures discussed later in the book. However, rather than starting directly with the discussion of this algorithm, we will start with something simpler: a children's book and some fundamental observations about machine learning. From these, we will formalize our first machine learning algorithm, the Perceptron. In the following chapters, we will improve upon the Perceptron with logistic regression (Chapter 3), and deeper feed forward neural networks (Chapter 5).

2.1 Machine Learning Is Easy

Machine learning is easy. To convince you of this, let us read a children's story [**?**]. The story starts with a little monkey that lost her mom in the jungle (Figure 2.1). Luckily, the butterfly offers to help, and collects some information about the mother from the little monkey (Figure 2.2). As a result, the butterfly leads the monkey to an elephant. The monkey explains that her mom is neither gray nor big, and does not have a trunk. Instead, her mom has a "tail that coils around trees". Their journey through the jungle continues until, after many mistakes (e.g., snake, spider), the pair end up eventually finding the monkey's mom, and the family is happily reunited.

In addition to the exciting story that kept at least a toddler and this parent glued to its pages, this book introduces several fundamental observations about (machine) learning.

First, *objects are described by their properties*, also known in machine learning terminology as *features*. For example, we know that several features apply to the monkey mom: `isBig`, `hasTail`, `hasColor`, `numberOfLimbs`, etc. These features have values, which may be Boolean (true or false), a discrete value from a fixed set, or a number. For example, the values for the above features are: `false`, `true`, `brown` (out of multiple possible colors), and 4. As we will see soon, it is preferable to convert these values into numbers because most of the machine learning can be reduced to numeric operations such as additions and multiplications. For this reason, Boolean features are converted to 0 for false, and 1 for true. Features that take discrete values are converted to Boolean features by enumerating over the possible values in the set. For example, the color feature is converted into a set of Boolean

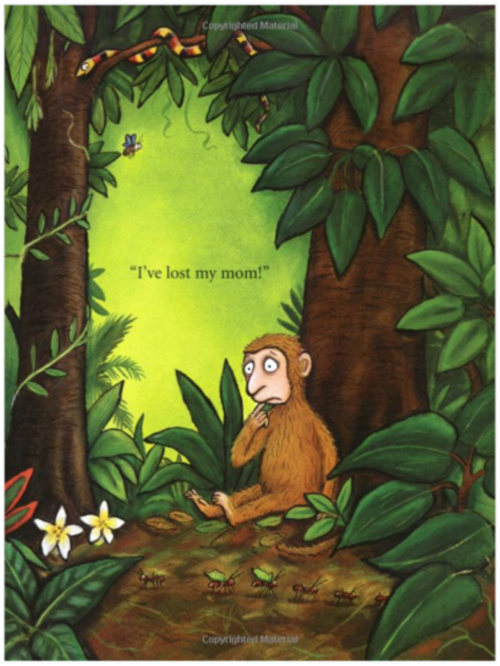

Figure 2.1 An exciting children's book that introduces the fundamentals of machine learning: Where's My Mom, by Julia Donaldson and Axel Scheffler [**?**].

features such as `hasColorBrown` with the value `true` (or 1), `hasColorRed` with the value `false` (or 0), etc.

Second, *objects are assigned a discrete label*, which the learning algorithm or *classifier* (the butterfly has this role in our story) will learn how to assign to new objects. For example, in our story we have two labels: `isMyMom` and `isNotMyMom`. When there are two labels to be assigned such as in our story, we call the problem at hand a *binary classification problem*. When there are more than two labels, the problem becomes a *classification task*. Sometimes, the labels are continuous numeric values, in which case the problem at hand is called a *regression task*. An example of such a regression problem would be learning to forecast the price of a house on the real estate market from its properties, e.g., number of bedrooms, and year it was built. However, in NLP most tasks are classification problems (we will see some simple ones in this chapter, and more complex ones starting with Chapter 12).

To formalize what we know so far, we can organize the examples the classifier has seen (also called a training dataset) into a matrix of features $\mathbf{X}$ and a vector of labels $\mathbf{y}$. Each example seen by the classifier takes a row in $\mathbf{X}$, with each of the features occupying a different

Little monkey: "I've lost my mom!"

"Hush, little monkey, don't you cry. I'll help you find her," said butterfly. "Let's have a think, How big is she?"

"She's big!" said the monkey. "Bigger than me."

"Bigger than you? Then I've seen your mom. Come, little monkey, come, come, come."

"No, no, no! That's an elephant."

Figure 2.2 The butterfly tries to help the little monkey find her mom, but fails initially [**?**]. TODO: check fair use!

Table 2.1 An example of a possible feature matrix **X** (left table) and a label vector **y** (right table) for three animals in our story: elephant, snake, and monkey.

isBig	hasTail	hasTrunk	hasColorBrown	numberOfLimbs
1	1	1	0	4
0	1	0	0	0
0	1	0	1	4

Label
isNotMyMom
isNotMyMom
isMyMom

column. Each y_i is the label of the corresponding example $\mathbf{x}_i$. Table 2.1 shows an example of a possible matrix **X** and label vector **y** for three animals in our story.

The third observation is that a good learning algorithm *aggregates its decisions over multiple examples with different features*. In our story the butterfly learns that some features are positively associated with the mom (i.e., she is likely to have them), while some are negatively associated with her. For example, from the animals the butterfly sees in the story, it learns that the mom is likely to have a tail, fur, and four limbs, and she is not big, does not have a trunk, and her color is not gray. We will see soon that this is exactly the intuition behind the simplest neural network, the Perceptron.

Lastly, learning algorithms produce incorrect classifications when not exposed to sufficient data. This situation is called *overfitting*, and it is more formally defined as the situation when an algorithm performs well in training (e.g., once the butterfly sees the snake, it will reliably classify it as not the mom when it sees in the future), but poorly on unseen data (e.g., knowing that the elephant is not the mom did not help much with the classification of the snake). To detect overfitting early, machine learning problems typically divide their data into three partitions: (a) a training partition from which the classifier learns; (b) a development partition that is used for the *internal* validation of the trained classifier, i.e., if it performs poorly on this dataset, the classifier has likely overfitted; and (c) a testing partition that is used *only* for the final, formal evaluation. Machine learning developers typically alternate between training (on the training partition) and validating what is being learned (on the development partition) until acceptable performance is observed. Once this is reached, the resulting classifier is evaluated (ideally once) on the testing partition.

2.2 Use Case: Text Classification

In the remaining of this chapter, we will begin to leave the story of the little monkey behind us, and change to a related NLP problem, text classification, in which a classifier is trained to assign a label to a text. This is an important and common NLP task. For example, email providers use binary text classification to classify emails into spam or not. Data mining companies use multiclass classification to detect how customers feel about a product, e.g., like, dislike, or neutral. Search engines use multiclass classification to detect the language a document is written in before processing it.

Throughout the next few chapters, we will focus on text classification for simplicity. We will consider only two labels for the next few chapters, and we will generalize the algorithms discussed to multiclass classification (i.e., more than two labels) in Chapter 6. After we discuss sequence models (Chapter 12), we will introduce more complex NLP tasks such as part-of-speech tagging and syntactic parsing.

For now, we will extract simple features from the texts to be classified. That is, we will simply use the frequencies of words in a text as its features. More formally, the matrix $\mathbf{X}$, which stores the entire dataset, will have as many columns as words in the vocabulary. Each cell x_{ij} corresponds to the number of times the word at column j occurs in the example stored at row i. For example, the text *This is a great great buy* will produce a feature corresponding to the word *buy* with value 1, one for the word *great* with value 2, etc., while the features corresponding to all the other words in the vocabulary that do not occur in this document receive a value of 0. This feature design strategy is often referred to as *bag of words*, because it ignores all the syntactic structure of the text, and treats the text simply as a collection of independent words. We will revisit this simplification in Chapter 12, where we will start to model sequences of words.

2.3 Evaluation Measures for Text Classification

The simplest evaluation measure for text classification is accuracy, defined as the proportion of evaluation examples that are correctly classified. For example, the accuracy of the hypothetical classifier shown in Table 2.2 is $3/5 = 60\%$ because the classifier was incorrect on two examples (rows 2 and 4).

Using the four possible outcomes for binary classification summarized in the matrix shown in Table 2.3, which is commonly referred to as a confusion matrix, accuracy can be more

Table 2.2 Example output of a hypothetical classifier on five evaluation examples and two labels: positive ($+$) and negative ($-$). The "Gold" column indicates the correct labels for the five texts; the "Predicted" column indicates the classifier's predictions.

	Gold	Predicted
1	$+$	$+$
2	$+$	$-$
3	$-$	$-$
4	$-$	$+$
5	$+$	$+$

Table 2.3 Confusion matrix showing the four possible outcomes in binary classification, where $+$ indicates the positive label and $-$ indicates the negative label.

	Classifier predicted $+$	Classifier predicted $-$
Gold label is $+$	True positive (TP)	False negative (FN)
Gold label is $-$	False positive (FP)	True negative (TN)

formally defined as:

$$\text{Accuracy} = \frac{TP+TN}{TP+FN+FP+TN} \tag{2.1}$$

For example, for the classifier output shown in Table 2.2, TP = 2 (rows 1 and 5), TN = 1 (row 3), FP = 1 (row 4), and FN = 1 (row 2).

While accuracy is obviously useful, it is not always informative. In problems where the two labels are heavily unbalanced, i.e., one is much more frequent than the other, and we care more about the less frequent label, a classifier that is not very useful may have a high accuracy score. For example, assume we build a classifier that identifies high-urgency Medicaid applications,[1] i.e., applications must be reviewed quickly due to the patient's medical condition. The vast majority of applications are not high-urgency, which means they can be handled through the usual review process. In this example, the positive class is assigned to the high-urgency applications. If a classifier labels all applications as negative (i.e., not high-urgency), its accuracy will be high because the TN count dominates the accuracy score. For example, say that out of 1,000 applications only 1 is positive. Our classifier's accuracy is then: $\frac{0+999}{0+1+0+999} = 0.999$, or 99.9%. This high accuracy is obviously misleading in any real-world application of the classifier.

[1] Medicaid is a federal and state program in the United States that helps with medical costs for some people with limited income and resources.

For such unbalanced scenarios, two other scores that focus on class of interest (say, the positive class) are commonly used: precision and recall. Precision (P) is the proportion of correct positive examples out of all positives predicted by the classifier. Recall (R) is the proportion of correct positive examples out of all positive examples in the evaluation dataset. More formally:

$$P = \frac{TP}{TP+FP} \tag{2.2}$$

$$R = \frac{TP}{TP+FN} \tag{2.3}$$

For example, both the precision and recall of the above classifier are 0 because $TP = 0$ in its output. On the other hand, a classifier that predicts 2 positives, out of which only one is incorrect, will have a precision of $1/2 = 0.5$ and a recall of $1/1 = 1$, which are clearly more informative of the desired behavior.

Often it helps to summarize the performance of a classifier using a single number. The F_1 score achieves this, as the harmonic mean of precision and recall:

$$F_1 = \frac{2PR}{P+R} \tag{2.4}$$

For example, the F1 score for the previous example is: $F_1 = \frac{2\times0.5\times1}{0.5+1} = 0.66$. A reasonable question to ask here is why not use instead the simpler arithmetic mean between precision and recall ($\frac{P+R}{2}$) to generate this overall score? The reason for choosing the more complicated harmonic mean is that this formula is harder to game. For example, consider a classifier that labels everything as positive. Clearly, this would be useless in the above example of classifying high-urgency Medicaid applications. This classifier would have a recall of 1 (because it did identify all the high-urgency applications), and a precision of approximately 0 (because everything else in the set of 1,000 applications is also labeled as high-urgency). The simpler arithmetic mean of the two scores is approximately 0.5, which is an unreasonably high score for a classifier that has zero usefulness in practice. In contrast, the F1 score of this classifier is approximately 0, which is more indicative of the classifier's overall performance. In general, the F_1 score penalizes situations where the precision and recall values are far apart from each other.

A more general form of the F1 score is:

$$F_\beta = (1+\beta^2)\frac{PR}{(\beta^2 P)+R} \tag{2.5}$$

where β is a positive real value, which indicates that recall is β times more important than precision. This generalized formula allows one to compute a single overall score for situations when precision and recall are not treated equally. For example, in the high-urgency Medicaid example, we may decide that recall is more important than precision. That is, we are willing to inspect more incorrect candidates for high-urgency processing as long as we do not miss the true positives. If we set $\beta = 10$ to indicate that we value recall as being 10 times more important than precision, the classifier in the above example ($P = 0.5$ and $R = 1$) has a $F_{\beta=10}$ score of: $F_{\beta=10} = 101\frac{0.5\times1}{(100\times0.5)+1} = 0.99$, which is much closer to the classifier's recall value (the important measure here) than the F_1 score.

We will revisit these measures in Chapter 3, where we will generalize them to multiclass classification, i.e., to situations where the classifier must produce more than two labels, and in Chapter 4, where we will implement and evaluate multiple text classification algorithms.

2.4 The Perceptron

Now that we understand our first NLP task, text classification, let us introduce our first classification algorithm, the Perceptron. The Perceptron was invented by Frank Rosenblatt in 1958. Its aim is to mimic the behavior of a single neuron [**?**]. Figure 2.3 shows a depiction of a biological neuron,[2] and Rosenblatt's computational simplification, the Perceptron. As the figure shows, the Perceptron is the simplest possible artificial neural network. We will generalize from this single-neuron architecture to networks with an arbitrary number of neurons in Chapter 5.

The Perceptron has one input for each feature of an example **x**, and produces an output that corresponds to the label predicted for **x**. Importantly, the Perceptron has a weight vector **w**, with one weight w_i for each input connection i. Thus, the size of **w** is equal to the number of features, or the number of columns in **X**. Further, the Perceptron also has a bias term, b, that is scalar (we will explain why this is needed later in this section). The Perceptron outputs a binary decision, let us say Yes or No (e.g., Yes, the text encoded in **x** contains a positive review for a product, or No, the review is negative), based on the decision function described in Algorithm 1. The $\mathbf{w} \cdot \mathbf{x}$ component of the decision function is called the *dot product* of the vectors **w** and **x**. Formally, the dot product of two vectors **x** and **y** is defined as:

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i \tag{2.6}$$

where n indicates the size of the two vectors. In words, the dot product of two vectors, **x** and **y**, is found by adding (Σ), the values found by multiplying each element of **x** with the corresponding value of **y**. In the case of the Perceptron, the dot product of **x** and **w** is the weighted sum of the feature values in **x**, where each feature value x_i is weighted by w_i. If this

[2] By BruceBlaus – Own work, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=28761830

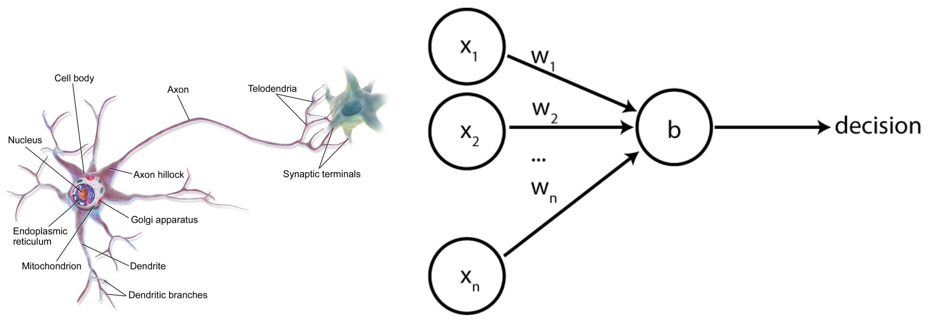

Figure 2.3 A depiction of a biological neuron, which captures input stimuli through its dendrites and produces an activation along its axon and synaptic terminals (left), and its computational simplification, the Perceptron (right).

Algorithm 1: The decision function of the Perceptron.

```
1 if $\mathbf{w} \cdot \mathbf{x} + b > 0$ then
2     return Yes
3 else
4     return No
5 end
```

sum (offset by the bias term b, which we will discuss later) is positive, then the decision is Yes. If it is negative, the decision is No.

Sidebar 2.1 The dot product in linear algebra

In linear algebra, the dot product of two vectors $\mathbf{x}$ and $\mathbf{y}$ is equivalent to $\mathbf{x}^T\mathbf{y}$, where T is the transpose operation. However, in this book we rely on the dot product notation for simplicity.

Sidebar 2.2 The sign function in the Perceptron

The decision function listed in Algorithm 1 is often shown as $\text{sign}(\mathbf{w} \cdot \mathbf{x} + b)$, where the $+$ sign is used to represent one class, and the $-$ sign the other.

There is an immediate parallel between this decision function and the story of the little monkey. If we consider the Yes class to be `isMyMom`, then we would like the weights of

Algorithm 2: Perceptron learning algorithm.

```
1  $\mathbf{w} = 0$
2  b = 0
3  while not converged do
4      for each training example $\mathbf{x}_i$ in X do
5          d = decision($\mathbf{x}_i$, $\mathbf{w}$, b)
6          if $d == y_i$ then
7              continue
8          else if $y_i == Yes$ and $d == No$ then
9              $b = b + 1$
10             $\mathbf{w} = \mathbf{w} + \mathbf{x}_i$
11         else if $y_i == No$ and $d == Yes$ then
12             $b = b - 1$
13             $\mathbf{w} = \mathbf{w} - \mathbf{x}_i$
14     end
15 end
```

the features that belong to the mom (e.g., `hasColorBrown`) to have positive values, so the dot product between **w** and the **x** vector corresponding to the mom turns out positive, and the features specific to other animals (e.g., `hasTrunk`) to receive negative weights, so the corresponding decision is negative. Similarly, if the task to be learned is review classification, we would like positive words (e.g., *good*, *great*) to have positive weights in **w**, and negative words (e.g., *bad*, *horrible*) to have negative weights.

In general, we call the aggregation of a learning algorithm or classifier and its learned parameters (**w** and b for the Perceptron) a *model*. All classifiers aim to learn these parameters to optimize their predictions over the examples in the training dataset.

The key contribution of the Perceptron is a simple algorithm that learns these weights (and bias term) from the given training dataset. This algorithm is summarized in Algorithm 2. Let us dissect this algorithm next. The algorithm starts by initializing the weights and bias term with 0s. Note that lines of pseudocode that assign values to a vector such as line 1 in the algorithm ($\mathbf{w} = 0$) assign this scalar value to *all* the elements of the vector. For example, the operation in line 1 initializes all the elements of the weight vector with zeros.

Lines 3 and 4 indicate that the learning algorithm may traverse the training dataset more than once. As we will see in the following example, sometimes this repeated exposure to training examples is necessary to learn meaningful weights. Informally, we say that the algorithm *converged* when there are no more changes to the weight vector (we will define convergence more formally later in this section). In practice, on real-world tasks, it is possible that true convergence is not reached, so, commonly, line 3 of the algorithm is written to limit the number of traversals of the training dataset (or *epochs*) to a fixed number.

Line 5 applies the decision function in Algorithm 1 to the current training example. Lines 6 and 7 indicate that the Perceptron simply skips over training examples that it already knows how to classify, i.e., its decision d is equal to the correct label y_i. This is intuitive: if the Perceptron has already learned how to classify an example, there is limited benefit in learning it again. In fact, the opposite might happen: the Perceptron weights may become too tailored for the particular examples seen in the training dataset, which will cause it to overfit. Lines 8 – 10 address the situation when the correct label of the current training example $\mathbf{x}_i$ is Yes, but the prediction according to the current weights and bias is No. In this situation, we would intuitively want the weights and bias to have higher values such that the overall dot product plus the bias is more likely to be positive. To move towards this goal, the Perceptron simply *adds* the feature values in $\mathbf{x}_i$ to the weight vector $\mathbf{w}$, and adds 1 to the bias. Similarly, when the Perceptron makes an incorrect prediction for the label No (lines 11 – 13), it decreases the value of the weights and bias by *subtracting* $\mathbf{x}_i$ from $\mathbf{w}$, and subtracting 1 from b.

Sidebar 2.3 Error driven learning

The class of algorithms such as the Perceptron that focus on "hard" examples in training, i.e., examples for which they make incorrect predictions at a given point in time, are said to perform *error driven learning*.

Figure 2.4 shows an intuitive visualization of this learning process.[3] In this figure, for simplicity, we are ignoring the bias term and assume that the Perceptron decision is driven solely by the dot product $\mathbf{x} \cdot \mathbf{w}$. Figure 2.4 (a) shows the weight vector $\mathbf{w}$ in a simple two-dimensional space, which would correspond to a problem that is represented using only two features.[4] In addition of $\mathbf{w}$, the figure also shows the *decision boundary* of the Perceptron as a dashed line that is perpendicular on $\mathbf{w}$. The figure indicates that all the vectors that lie on the same side of the decision boundary with $\mathbf{w}$ are assigned the label Yes, and all the vectors on the other side receive the decision No. Vectors that lie exactly on the decision boundary (i.e., their decision function has a value of 0) receive the label No according to Algorithm 1. In the transition from (a) to (b), the figure also shows that redrawing the boundary changes the decision for $\mathbf{x}$.

[3] This visualization was first introduced by **?**.

[4] This simplification is useful for visualization, but it is highly unrealistic for real-world NLP applications, where the number of features is often proportional with the size of a language's vocabulary, i.e., it is often in the hundreds of thousands.

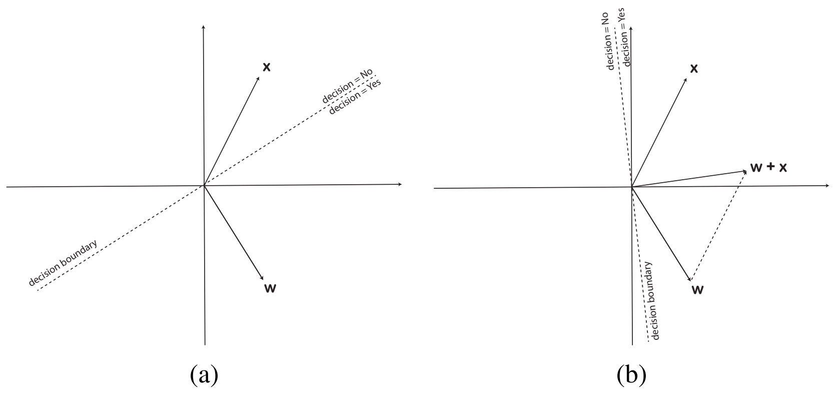

Figure 2.4 Visualization of the Perceptron learning algorithm: (a) incorrect classification of the vector **x** with the label Yes, for a given weight vector **w**; and (b) **x** lies on the correct side of the decision boundary after **x** is added to **w**.

Why is the decision boundary line perpendicular on **w**, and why are the labels so nicely assigned? To answer these questions, we need to introduce a new formula that measures the cosine of the angle between two vectors, *cos*:

$$cos(\mathbf{x},\mathbf{y}) = \frac{\mathbf{x}\cdot\mathbf{y}}{||\mathbf{x}||||\mathbf{y}||} \tag{2.7}$$

where $||\mathbf{x}||$ indicates the length of vector **x**, i.e., the distance between the origin and the tip of the vector's arrow, measured with a generalization of Pythagoras's theorem:[5] $||\mathbf{x}|| = \sqrt{\sum_{i=1}^{N} x_i^2}$. The cosine similarity, which ranges between -1 and 1, is widely used in the field of information retrieval to measure the similarity of two vectors [**?**]. That is, two perfectly similar vectors will have an angle of 0° between them, which has the largest possible cosine value of 1. Two "opposite" vectors have an angle of 180° between them, which has a cosine of -1. We will extensively use the cosine similarity formula starting with the next chapter. But, for now, we will simply observe that the cosine similarity value has the same sign with the dot product of the two vectors (because the length of a vector is always positive). Because vectors on the same side of the decision boundary with **w** have an angle with **w** in the interval [$-90°$, $90°$], the corresponding cosine (and, thus, dot product value) will be positive, which yields a

[5] Pythagoras's theorem states that the square of the hypothenuse, c, of a right triangle is equal to the sum of the squares of the other two sides, a and b, or, equivalently: $c = \sqrt{a+b}$. In our context, c is the length of a vector with coordinates a and b in a two-dimensional space.

Table 2.4 The feature matrix **X** (left table) and label vector **y** (right table) for a review classification training dataset with three examples.

#	*good*	*excellent*	*bad*	*horrible*	*boring*
#1	1	1	1	0	0
#2	0	0	1	1	0
#3	0	0	1	0	1

Label
Positive
Negative
Negative

Yes decision. Similarly, vectors on the other side of the decision boundary will receive a No decision.

Sidebar 2.4 Hyper planes and Perceptron convergence

In a one-dimensional feature space, the decision boundary for the Perceptron is a dot. As shown in Figure 2.4, in a two-dimensional space, the decision boundary is a line. In a three-dimensional space, the decision boundary is a plane. In general, for a n-dimensional space, the decision boundary of the Perceptron is a *hyper plane*. Classifiers such as the Perceptron whose decision boundary is a hyper plane, i.e., it is driven by a linear equation in **w** (see Algorithm 1), are called *linear classifiers*.

If such a hyper plane that separates the labels of the examples in the training dataset exists, it is guaranteed that the Perceptron will find it, or will find another hyper plane with similar separating properties [**??**]. We say that the learning algorithm has *converged* when such a hyper plane is found, which means that all examples in the training data are correctly classified.

Figure 2.4 (a) shows that, at that point in time, the training example **x** with label Yes lies on the incorrect side of the decision boundary. Figure 2.4 shows how the decision boundary is adjusted after **x** is added to **w** (line 10 in Algorithm 2). After this adjustment, **x** is on the correct side of the decision boundary.

To convince ourselves that the Perceptron is indeed learning a meaningful decision boundary, let us go trace the learning algorithm on a slightly more realistic example. Table 2.4 shows the matrix **X** and label vector **y** for a training dataset that contains three examples for a product review classification task. In this example, we assume that our vocabulary has only the five words shown in **X**, e.g., the first data point in this dataset is a positive review that contains the words *good*, *excellent*, and *bad*.

Table 2.5 traces the learning algorithm as it iterates through the training examples. For example, because the decision function produces the incorrect decision for the first example (No), this example is added to **w**. Similarly, the second example is subtracted from **w**. The

Table 2.5 The Perceptron learning process for the dataset shown in Table 2.4, for one pass over the training data. Both $\mathbf{w}$ and b are initialized with 0s.

Example seen: #1
$\mathbf{x} \cdot \mathbf{w} + b = 0$
Decision = Negative
Update (add): $\mathbf{w} = (1, 1, 1, 0, 0)$, $b = 1$
Example seen: #2
$\mathbf{x} \cdot \mathbf{w} + b = 2$
Decision = Positive
Update (subtract): $\mathbf{w} = (1, 1, 0, -1, 0)$, $b = 0$
Example seen: #3
$\mathbf{x} \cdot \mathbf{w} + b = 0$
Decision = Negative
Update: none

third example is correctly classified (barely), so no update is necessary. After just one pass over this training dataset, also called an *epoch*, the Perceptron has converged. We will let the reader convince herself that all training examples are now correctly classified. The final weights indicate that the Perceptron has learned several useful things. First, it learned that *good* and *excellent* are associated with the Yes class, and has assigned positive weights to them. Second, it learned that *bad* is not to be trusted because it appears in both positive and negative reviews, and, thus, it assigned it a weight of 0. Lastly, it learned to assign a negative weight to *horrible*. However, it is not perfect: it did not assign a non-zero weight to *boring* because of the barely correct prediction made on example #3. There are other bigger problems here. We discuss them in Section 2.7.

This example as well as Figure 2.4 seem to suggest that the Perceptron learns just fine without a bias term. So why do we need it? To convince ourselves that the bias term is useful let us walk through another simple example, shown in Table 2.6. The Perceptron needs four epochs, i.e., four passes over this training dataset, to converge. The final parameters are: $\mathbf{w} = (2)$ and $b = -4$. We encourage the reader to trace the learning algorithm through this dataset on her own as well. These parameters indicate that the hyper plane for this Perceptron, which is a dot in this one-dimensional feature space, is at 2 (because the final inequation for the positive decision is $2x - 4 > 0$). That is, in order to receive a Yes decision, the feature of the corresponding example must have a value > 2, i.e., the review must have at least three positive words. This is intuitive, as the training dataset contains negative reviews that contain one or two positive words. What this shows is that the bias term allows the Perceptron to shift its decision boundary *away* from the origin. It is easy to see that, without a bias term,

Table 2.6 The feature matrix **X** (left table) and label vector **y** (right table) for a review classification training dataset with four examples. In this example, the only feature available is the *total* number of positive words in a review.

#	Number of positive words
#1	1
#2	10
#3	2
#4	20

Label
Negative
Positive
Negative
Positive

the Perceptron would not be able to learn anything meaningful, as the decision boundary will always be in the origin. In practice, the bias term tends to be more useful for problems that are modeled with few features. In real-world NLP tasks that are high-dimensional, learning algorithms usually find good decision boundaries even without a bias term (because there are many more options to choose from).

Sidebar 2.5 Implementations of the bias term

Some machine learning software packages implement the bias term as an additional feature in $\mathbf{x}$ that is always active, i.e., it has a value of 1 for all examples in $\mathbf{X}$. This simplifies the math a bit, i.e., instead of computing $\mathbf{x} \cdot \mathbf{w} + b$, we now have to compute just $\mathbf{x} \cdot \mathbf{w}$. It is easy to see that modeling the bias as an always-active feature has the same functionality as the explicit bias term in Algorithm 2. In this book, we will maintain an explicit bias term for clarity.

2.5 Voting Perceptron

As we saw in the previous examples, the Perceptron learns well, but it is not perfect. Often, a very simple strategy to improve the quality of classifier is to use an *ensemble model*. One such ensemble strategy is to *vote* between the decisions of multiple learning algorithms. For example, Figure 2.5 shows a visualization of such a voting Perceptron, which aggregates two individual Perceptrons by requiring that both classifiers label an example as $\times$ before issuing the $\times$ label.[6]

The figure highlights two important facts. First, the voting Perceptron performs better than either individual classifier. In general, ensemble models that aggregate models that are sufficiently different from each other tend to perform better than the individual (or base) classifiers that are part of the ensemble [**?**]. Second, and more important for our discussion, the voting Perceptron is a *non-linear classifier*, i.e., its decision boundary is no longer a line (or

[6] This example taken from Erwin Chan's Ling 539 course at University of Arizona.

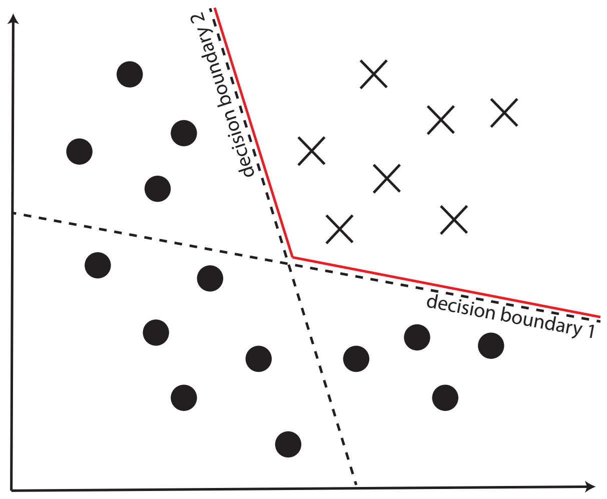

Figure 2.5 An example of a binary classification task, and a voting Perceptron that aggregates two imperfect Perceptrons. The voting algorithm classifies correctly all the data points by requiring two votes for the $\times$ class to yield a $\times$ decision. The decision boundary of the voting Perceptron is shown in red.

a hyper plane in n dimensions). In figure 2.5, the decision boundary for the voting Perceptron is shown with the red lines.

While the voting approach is an easy way to produce a non-linear classifier that improves over the basic Perceptron, it has drawbacks. First, we need to produce several individual Perceptron classifiers. This can be achieved in at least two distinct ways. For example, instead of initializing the $\mathbf{w}$ and b parameters with 0s (lines 1 and 2 in Algorithm 2), we initialize them with random numbers (typically small numbers centered around 0). For every different set of initial values in $\mathbf{w}$ and b, the resulting Perceptron will end up with a different decision boundary, and, thus, a different classifier. The drawback of this strategy is that the training procedure must be repeated for each individual Perceptron. A second strategy for producing multiple individual Perceptron that avoids this training overhead is to keep track of all $\mathbf{w}$s and bs that are produced during the training of a single Perceptron. That is, before changing the b and $\mathbf{w}$ parameters in Algorithm 2 (lines 9 and 12), we store the current values (before the change) in a list. This means that at the end of the training procedure, this list will contain as many individual Perceptrons as the number of updates performed in training. We can even sort these individual classifiers by their perceived quality: the more iterations a specific b and $\mathbf{w}$ combination "survived" in training, the better the quality of this classifier is likely to be. This indicator of quality can be used to assign weights to the "votes" given to the individual classifiers, or to filter out base models of low quality (e.g., remove all classifiers that survived fewer than 10 training examples).

The second drawback of the voting Perceptron is its runtime overhead at evaluation time. When the voting Perceptron is applied on a new, unseen example, it must apply all its individual classifiers before voting. Thus, the voting Perceptron is N times slower than the individual Perceptron, where N is the number of individual classifiers used. To mitigate this drawback, we will need the average Perceptron, discussed next.

2.6 Average Perceptron

The average Perceptron is a simplification of the latter voting Perceptron discussed previously. The simplification consists in that, instead of keeping track of *all* $\mathbf{w}$ and b parameters created during the Perceptron updates like the voting algorithm, these parameters are averaged into a *single* model, say **avgW** and $avgB$. This algorithm, which is summarized in Algorithm 3, has a constant runtime overhead for computing the average model, i.e., the only additional overhead compared to the regular Perceptron are the additions in lines 12 – 14 and 18 – 20, and the divisions in lines 25 and 26. Further, the additional memory overhead is also constant, as it maintains a single extra weight vector (**totalW**) and a single bias term ($totalB$) during training. After training, the average Perceptron uses a decision function different from the one used during training. This function has a similar shape to the one listed in Algorithm 1, but uses **avgW** and $avgB$ instead.

Despite its simplicity, the average Perceptron tends to perform well in practice, usually outperforming the regular Perceptron, and approaching the performance of the voting Perceptron. But why is the performance of the average Perceptron so good? After all, it remains a linear classifier just like the regular Perceptron, so it must have the same limitations. The intuitive explanation for its good performance is the following. When the Perceptron is exposed to unreliable features during training, these features will receive weight values in the Perceptron model (the $\mathbf{w}$ vector) that are all over the place, sometimes positive and sometimes negative. All these values are averaged in the average vector, and, thus, the average weight value for these unreliable features will tend to be squished to zero. The effect of this squishing to zero is that the decision function of the average Perceptron will tend to not rely on these features (because their contribution to the dot product in the decision function will be minimal). This differs from the regular Perceptron, which does not benefit from this averaging process that reduces the weights of unimportant features. In general, this process of squishing to zero the weights of features that are not important is called *regularization*. We will see other regularization strategies starting with the logistic regression classifier, in the next chapter.

2.7 Drawbacks of the Perceptron

The Perceptron algorithm and its variants are simple, easy to customize for other tasks beyond text classification, and they perform fairly well (especially in the voting and average form).

Algorithm 3: Average Perceptron learning algorithm.

```
w = 0
b = 0
numbertotalOfUpdates = 0
totalW = 0
totalB = 0
while not converged do
    for each training example $\mathbf{x_i}$ in X do
        d = decision($\mathbf{x_i}$, $\mathbf{w}$, b)
        if $d == y_i$ then
            continue
        else if $y_i == Yes$ and $d == No$ then
            $\text{numberOfUpdates} = \text{numberOfUpdates} + 1$
            $\textbf{totalW} = \textbf{totalW} + \mathbf{w}$
            $\text{totalB} = \text{totalB} + b$
            $\mathbf{w} = \mathbf{w} + \mathbf{x_i}$
            $b = b + 1$
        else if $y_i == No$ and $d == Yes$ then
            $\text{numberOfUpdates} = \text{numberOfUpdates} + 1$
            $\textbf{totalW} = \textbf{totalW} + \mathbf{w}$
            $\text{totalB} = \text{totalB} + b$
            $\mathbf{w} = \mathbf{w} - \mathbf{x_i}$
            $b = b - 1$
    end
end
$\text{avgB} = \text{totalB}/\text{numberOfUpdates}$
$\textbf{avgW} = \textbf{totalW}/\text{numberOfUpdates}$
```

However, they also have important drawbacks. We discuss these drawbacks here, and we will spend a good part of this book discussing solutions that address them.

The first obvious limitation of the Perceptron is that, as discussed in this chapter, it is a linear classifier. Yes, the voting Perceptron removes this constraint, but it comes at the cost of maintaining multiple individual Perceptrons. Ideally, we would like to have the ability to learn a single classifier that captures a non-linear decision boundary. This ability is important, as many tasks require such a decision boundary. A simple example of such a task was discussed by Minsky and Papert as early as 1969: the Perceptron cannot learn the XOR function [**?**].

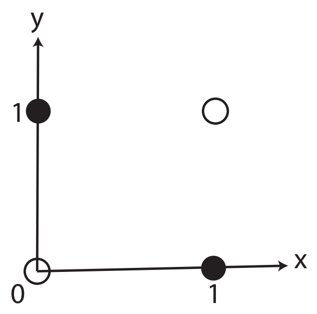

Figure 2.6 Visualization of the XOR function operating over two variables, *x* and *y*. The dark circles indicate that the XOR output is 1; the clear circles stand for 0.

To remind ourselves, the XOR function takes two binary variables, i.e., numbers that can take only one of two values: 0 (which stands for False) or 1 (or True), and outputs 1 when exactly one of these values is 1, and 0 otherwise. A visualization of the XOR is shown in Figure 2.6. It is immediately obvious that there is no linear decision boundary that separates the dark circles from the clear ones. More importantly in our context, language is beautiful, complex, and ambiguous, which means that, usually, we cannot model tasks that are driven by language using methods of limited power such as linear classifiers. We will address this important limitation in Chapter 5, where we will introduce neural networks that can learn non-linear decision boundaries by combining multiple layers of "neurons" into a single network.

A second more subtle but very important limitation of the Perceptron is that it has no "smooth" updates during training, i.e., its updates are the same regardless of how incorrect the current model is. This is caused by the decision function of the Perceptron (Algorithm 1), which relies solely on the *sign* of the dot product. That is, it does not matter how large (or small) the value of the dot product is; when the sign is incorrect, the update is the same: adding or subtracting the *entire* example $\mathbf{x_i}$ from the current weight vector (lines 10 and 13 in Algorithm 2). This causes the Perceptron to be a slow learner because it jumps around good solutions. One University of Arizona student called this instability "Tony Hawk-ing the data".[7] On data that is linearly separable, the Perceptron will eventually converge [**?**]. However, real-world datasets do not come with this guarantee of linear separation, which means that this "Tony Hawk-ing" situation may yield a Perceptron that is far from acceptable. What we would like to have is a classifier that updates its model *proportionally* with the errors it makes: a small mistake causes a small update, while a large one yields a large update. This is exactly what the logistic regression does. We detail this in the next chapter.

[7] Tony Hawk is an American skateboarder, famous for his half-pipe skills. See: https://en.wikipedia.org/wiki/Tony_Hawk.

The third drawback of the Perceptron, as we covered it so far, is that it relies on hand-crafted features that must be designed and implemented by the machine learning developer. For example, in the text classification use case introduced in Section 2.2, we mentioned that we rely on features that are simply the words in each text to be classified. Unfortunately, in real-world NLP applications feature design gets complicated very quickly. For example, if the task to be learned is review classification, we should probably capture negation. Certainly the phrase *great* should be modeled differently than *not great*. Further, maybe we should investigate the syntactic structure of the text to be classified. For example, reviews typically contain multiple clauses, whose sentiment must be composed into an overall classification for the entire review. For example, the review *The wait was long, but the food was fantastic.* contains two clauses: *The wait was long* and *but the food was fantastic*, each one capturing a different sentiment, which must be assembled into an overall sentiment towards the corresponding restaurant. Further, most words in any language tend to be very infrequent [**?**], which means that a lot of the hard work we might invest in feature design might not generalize enough. That is, suppose that the reviews included in a review classification training dataset contain the word *great* but not the word *fantastic*, a fairy similar word in this context. Then, any ML algorithm that uses features that rely on explicit words will correctly learn how to associate *great* with a specific sentiment, but will not know what to do when they see the word *fantastic*. Chapter 8 addresses this limitation. We will discuss methods to transform words into a numerical representation that captures (some) semantic knowledge. Under this representation, similar words such as *great* and *fantastic* will have similar forms, which will improve the generalization capability of our ML algorithms.

Lastly, in this chapter we focused on text classification applications such as review classification that require a simple ML classifier, which produces a single binary label for an input text, e.g., positive vs. negative review. However, many NLP applications require multiclass classification (i.e., more than two labels), and, crucially, produce *structured* output. For example, a part-of-speech tagger, which identifies which words are nouns, verbs, etc., must produce the *sequence* of part of speech tags for a given sentence. Similarly, a syntactic parser identifies syntactic structures in a given sentence such as which phrase serves as subject for a given verb. These structures are typically represented as *trees*. The type of ML algorithms that produce structures rather than individual labels are said to perform *structured learning*. We will begin discussing structured learning in Chapter 12.

2.8 Historical Background

TODO: To do

2.9 References and Further Readings

TODO: To do

3 Logistic Regression

As mentioned in the previous chapter, the Perceptron does not perform smooth updates during training, which may slow down learning, or cause it to miss good solutions entirely in real-world situations. In this chapter, we will discuss logistic regression (LR), a machine learning algorithm that elegantly addresses this problem.

3.1 The Logistic Regression Decision Function and Learning Algorithm

As we discussed, the lack of smooth updates in the training of the Perceptron is caused by its reliance on a discrete decision function driven by the sign of the dot product. The first thing LR does is replace this decision function with a new, *continuous* function, which is:

$$\text{decision}(\mathbf{x}, \mathbf{w}, b) = \frac{1}{1 + e^{-(\mathbf{w} \cdot \mathbf{x} + b)}} \tag{3.1}$$

The $\frac{1}{1+e^{-x}}$ function is known as the logistic function, hence the name of the algorithm. The logistic function belongs to a larger class of functions called sigmoid functions because they are characterized by an S-shaped curve. Figure 3.1 shows the curve of the logistic function. In practice, the name sigmoid (or σ) is often used instead of logistic, which is why the LR decision function is often summarized as: $\sigma(\mathbf{w} \cdot \mathbf{x} + b)$. For brevity, we will use the σ notation in our formulas as well.

Figure 3.1 shows that the logistic function has values that monotonically increase from 0 to 1. We will use this property to implement a better learning algorithm, which has "soft" updates that are proportional to how incorrect the current model is. To do this, we first arbitrarily associate one of the labels to be learned with the value 1, and the other with 0. For example, for the review classification task, we (arbitrarily) map the positive label to 1, and the negative label to 0. Intuitively, we would like to learn a decision function that produces values close to 1 for the positive label, and values close to 0 for the negative one. The difference between the value produced by the decision function and the gold value for a training example will quantify the algorithm's confusion at a given stage in the learning process.

Algorithm 4 lists the LR learning process that captures the above intuitions. We will discuss later in this chapter how this algorithm was derived. For now, let us make sure that this algorithm does indeed do what we promised.

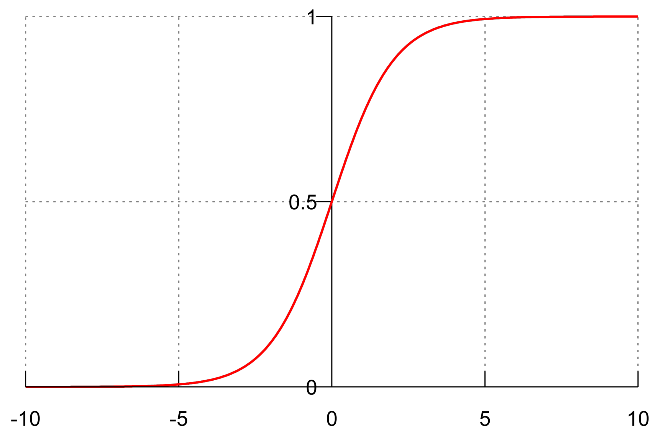

Figure 3.1 The sigmoid curve.

Note that the only new variable in this algorithm is α, known as the learning rate. The learning rate takes a positive value that adjusts up or down the values used during the update. We will revisit this idea later on in this chapter. For now, let us assume $\alpha = 1$.

It is easy to see that, at the extreme (i.e., when the prediction is perfectly correct or incorrect), this algorithm reduces to the Perceptron learning algorithm. For example, when the prediction is perfectly correct (say $y_i = 1$ for the class associated with 1), y_i is equal to d, which means that there is no weight or bias update in lines 6 and 7. This is similar to the Perceptron (lines 6 and 7 in Algorithm 2). Further, when a prediction is perfectly incorrect, say, $y_i = 1$ (Yes) when $d = 0$ (No), this reduces to adding $\mathbf{x}_i$ to $\mathbf{w}$ and 1 to b (similar to the Perceptron update, lines 8 – 10 in Algorithm 2). When $y_i = 0$ when $d = 1$, the algorithm reduces to subtracting $\mathbf{x}_i$ from $\mathbf{w}$ and 1 from b (similar to lines 11 – 13 in Algorithm 2).

The interesting behavior occurs in the majority of the situations when the LR decision is neither perfectly correct nor perfectly incorrect. In these situations, the LR performs a soft update that is proportional with how incorrect the current decision is, which is captured by $\mathrm{y}_i - \mathrm{d}$. That is, the more incorrect the decision is, the larger the update. This is exactly what we would like a good learning algorithm to do.

Once the algorithm finishes training, we would like to use the learned weights ($\mathbf{w}$ and b) to perform binary classification, e.g., classify a text into a positive or negative review. For this, at prediction time we will convert the LR decision into a discrete output using a threshold τ, commonly set to 0.5.[1] That is, if $\text{decision}(\mathbf{x}, \mathbf{w}, b) \geq 0.5$ then the algorithm outputs one class (say, positive review); otherwise it outputs the other class.

[1] Other values for this threshold are possible. For example, for applications where it is important to be conservative with predictions for class 1, τ should would take values larger than 0.5.

Algorithm 4: Logistic regression learning algorithm.

```
w = 0
b = 0
while not converged do
    for each training example $\mathbf{x}_i$ in X do
        d = decision($\mathbf{x}_i$, $\mathbf{w}$, b)
        $\mathbf{w} = \mathbf{w} + \alpha(\mathrm{y}_i - \mathrm{d})\mathbf{x}_i$
        $b = b + \alpha(\mathrm{y}_i - \mathrm{d})$
    end
end
```

3.2 The Logistic Regression Cost Function

The next three sections of this chapter focus on deriving the LR learning algorithm shown in Algorithm 4. The reader who is averse to math, or is satisfied with the learning algorithm and the intuition behind it, may skip to Section 3.7. However, we encourage the reader to try to stay with us through this derivation. These sections introduce important concepts, i.e., cost functions and gradient descent, which are necessary for a thorough understanding of the following chapters in this book. We will provide pointers to additional reading, where more mathematical background may be needed.

The first observation that will help us formalize the training process for LR is that the LR decision function implements a conditional probability, i.e., the probability of generating a specific label given a training example and the current weights. More formally, we can write:

$$p(y = 1|\mathbf{x}; \mathbf{w}, b) = \sigma(\mathbf{x}; \mathbf{w}, b) \tag{3.2}$$

The left term of the above equation can be read as the probability of generating a label y equal to 1, given a training example $\mathbf{x}$ and model weights $\mathbf{w}$ and b (the vertical bar "|" in the conditional probability formula should be read as "given"). Intuitively, this probability is an indicator of confidence (the higher the better). That is, the probability approaches 1 when the model is confident that the label for $\mathbf{x}$ is 1, and 0 when not. Similarly, the probability of y being 0 is:

$$p(y = 0|\mathbf{x}; \mathbf{w}, b) = 1 - \sigma(\mathbf{x}; \mathbf{w}, b) \tag{3.3}$$

These probabilities form a probability distribution, i.e., the sum of probabilities over all possible labels equals 1. Note that while we aim to minimize the use of probability theory in this section, some of it is unavoidable. The reader who wants to brush up on probability theory may consult other material on this topic such as [**?**].

To simplify notations, because in many cases it is obvious what the model weights are, we will skip them and use simply $p(y=1|\mathbf{x})$ and $p(y=0|\mathbf{x})$. Further, we generalize the above two formulas to work for any of the two possible labels with the following formula:

$$p(y|\mathbf{x}) = (\sigma(\mathbf{x};\mathbf{w},b))^y(1-\sigma(\mathbf{x};\mathbf{w},b))^{1-y} \tag{3.4}$$

It is trivial to verify that this formula reduces to one of the two equations above, for $y=1$ and $y=0$.

Intuitively, we would like the LR training process to maximize the probability of the correct labels in the entire training dataset. This probability is called the *likelihood of the data* (L), and is formalized as:

$$\begin{aligned} L(\mathbf{w},b) &= p(\mathbf{y}|\mathbf{X}) && (3.5)\\ &= \Pi_{i=1}^{m} p(y_i|\mathbf{x}_i) && (3.6) \end{aligned}$$

where $\mathbf{y}$ is the vector containing all the correct labels for all training examples, $\mathbf{X}$ is the matrix that contains the vectors of features for all training examples, and m is the total number of examples in the training dataset. Note that the derivation into the product of individual probabilities is possible because we assume that the training examples are independent of each other, and the joint probability of multiple independent events is equal to the product of individual probabilities [**?**].

A common convention in machine learning is that instead of maximizing a function during learning, we instead aim to minimize a *cost* or *loss* function C, which captures the amount of errors in the model. By definition, C must take only positive values. That is, C will have large values when the model does not perform well, and is 0 when the learned model is perfect. We write the logistic regression cost function C in terms of likelihood L as:

$$\begin{aligned} C(\mathbf{w},b) &= -\log L(\mathbf{w},b) && (3.7)\\ &= -\sum_{i=1}^{m}(y_i \log\sigma(\mathbf{x}_i;\mathbf{w},b) + (1-y_i)\log(1-\sigma(\mathbf{x}_i;\mathbf{w},b))) && (3.8) \end{aligned}$$

Equation 3.7 is often referred to as the *negative log likelihood* of the data. It is easy to see that C satisfies the constraints of a cost function. First, it is always positive: the logarithm of a number between 0 and 1 is negative; the negative sign in front of the sum turns the value of the sum into a positive number. Second, the cost function takes large values when the model

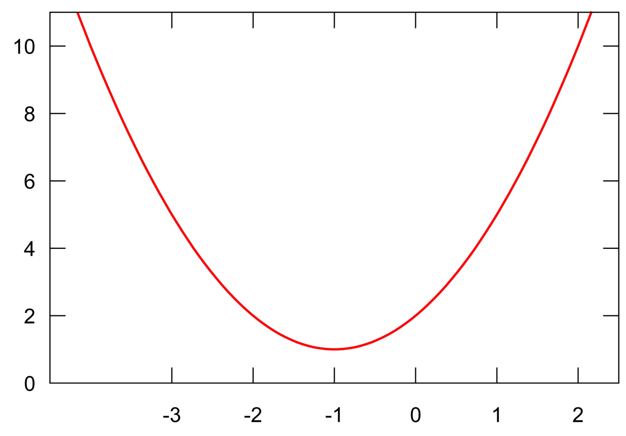

Figure 3.2 Plot of the function $f(x) = (x+1)^2 + 1$.

makes many mistakes (i.e., the likelihood of the data is small), and approaches 0 when the model is correct (i.e., the likelihood approaches 1).

Thus, we can formalize the goal of the LR learning algorithm as minimizing the above cost function. Next we will discuss how we do this efficiently.

3.3 Gradient Descent

The missing component that connects the cost function just introduced with the LR training algorithm (Algorithm 4) is gradient descent. Gradient descent is an iterative method that finds the parameters that minimize a given function. In our context, we will use gradient descent to find the LR parameters ($\mathbf{w}$ and b) that minimize the cost function C.

However, for illustration purposes, let us take a step away from the LR cost function and begin with a simpler example: let us assume we would like to minimize the function $f(x) = (x+1)^2 + 1$, which is plotted in Figure 3.2. Clearly, the smallest value this function takes is 1, which is obtained when $x = -1$. Gradient descent finds this value by taking advantage of the function slope, or derivative of $f(x)$ with respect to x, i.e., $\frac{d}{dx} f(x)$. Note: if the reader needs a refresher of what function derivatives are, and how to compute them, now is a good time to do so. Any calculus textbook or even the Wikipedia page for function derivatives[2] provide sufficient information for what we need in this book.

One important observation about the slope of a function is that it indicates the function's direction of change. That is, if the derivative is negative, the function decreases; if it is positive, the function increases; and if it is zero, we have reached a local minimum or maximum for the

[2] https://en.wikipedia.org/wiki/Derivative

function. Let us verify that is the case for our simple example. The derivative of our function $\frac{d}{dx}((x+1)^2+1)$ is $2(x+1)$, which has negative values when $x<-1$, positive values when $x>-1$, and is 0 when $x=-1$. Intuitively, gradient descent uses this observation to take small steps towards the function's minimum in the opposite direction indicated by the slope. More formally, gradient descent starts by initializing x with some random value, e.g., $x=-3$, and then repeatedly subtracts a quantity proportional with the derivative from x, until it *converges*, i.e., it reaches a derivative of 0 (or close enough so we can declare success). That is, we repeatedly compute:

$$x = x - \alpha \frac{d}{dx} f(x) \tag{3.9}$$

until convergence.

Sidebar 3.1 Partial derivative notation

In this book we use the Leibniz notation for derivatives. That is, $\frac{d}{dx}f$ indicates the derivative of function f with respect to x, i.e., the amount of change in f in response to an infinitesimal change in x. This notation is equivalent to the Lagrange notation (sometimes attributed to Newton) of $f'(x)$.

α in the above equation is the same learning rate introduced before in this chapter. Let us set $\alpha = 0.1$ for this example. Thus, in the first gradient descent iteration, x changes to $x = -3 - 0.1 \times 2(-3+1) = -2.6$. In the second iteration, x becomes $x = -2.6 - 0.1 \times 2(-2.6+1) = -2.28$. And so on, until, after approximately 30 iterations, x approaches -1.001, a value practically identical to what we were looking for.

This simple example also highlights that the learning rate α must be positive (so we don't change the direction indicated by the slope), and small (so we do not "Tony Hawk" the data). To demonstrate the latter situation, consider the situation when $\alpha = 1$. In this case, in the first iteration x becomes 1, which means we already skipped over the value that yields the function's minimum ($x=-1$). Even worse, in the second iteration, x goes back to -3, and we are now in danger of entering an infinite loop! To mitigate this situation, α usually takes small positive values, say, between 0.00001 and 0.1. In Chapter 6 we will discuss other strategies to dynamically shrink the learning rate as the learning advances, so we further reduce our chance of missing the function's minimum.

The gradient descent algorithm generalizes to functions with multiple parameters: we simply update each parameter using its own partial derivative of the function to be minimized. For example, consider a new function that has two parameters, x_1 and x_2: $f(x_1,x_2) = (x_1+1)^2+3x_2+1$. For this function, in each gradient descent iteration, we perform the following updates:

$$
\begin{aligned}
x_1 &= x_1 - \alpha \frac{d}{dx_1} f(x_1, x_2) = x_1 - 0.1(2x_1 + 2) \\
x_2 &= x_2 - \alpha \frac{d}{dx_2} f(x_1, x_2) = x_2 - 0.1(3)
\end{aligned}
$$

or, in general, for a function $f(\mathbf{x})$, we update each parameter x_i using the formula:

$$x_i = x_i - \alpha \frac{d}{dx_i} f(\mathbf{x}) \tag{3.10}$$

One obvious question that should arise at this moment is why are we not simply solving the equation where the derivative equals 0, as we were taught in calculus? For instance, for the first simple example we looked at, $f(x) = (x+1)^2 + 1$, zeroing the derivative yields immediately the exact solution $x = -1$. While this approach works well for functions with a single parameter or two, it becomes prohibitively expensive for functions with four or more parameters. Machine learning in general falls in this latter camp: it is very common that the functions we aim to minimize have thousands (or even millions) of parameters. In contrast, as we will see later, gradient descent provides a solution whose runtime is linear in the number of parameters times the number of training examples.

It is important to note that gradient descent is not perfect. It does indeed work well for convex functions, i.e., functions that have exactly one minimum and are differentiable at every point such as our simple example, but it does not perform so well in more complex situations. Consider for example the function shown in Figure 3.3.[3] This functions has two minima (around $x = 3$ and $x = -2$). Because gradient descent is a "greedy" algorithm, i.e., it commits to a solution relying only on local knowledge without understanding the bigger picture, it may end up finding a minimum that is not the best. For example, if x is initialized with 2.5, gradient descent will follow the negative slope at that position, and end up discovering the minimum around $x = 3$, which is not the best solution. However, despite this known limitation, gradient descent works surprisingly well in practice.

Now that we have a general strategy for finding the parameters that minimize a function, let us apply it to the problem we care about in this chapter, that is, finding the parameters $\mathbf{w}$ and b that minimize the cost function $C(\mathbf{w}, b)$ (Equation 3.8). A common source of confusion here is that the parameters of C are $\mathbf{w}$ and b, not $\mathbf{x}$ and y. For a given training example, $\mathbf{x}$ and y are known and constant. That is, we know the values of the features and the label for each given example in training, and all we have to do is compute $\mathbf{w}$ and b. Thus, the training process of LR reduces to repeatedly updating each w_j in $\mathbf{w}$ and b features by the corresponding partial derivative of C:

[3] This example of a function with multiple minima taken from https://en.wikipedia.org/wiki/Derivative.

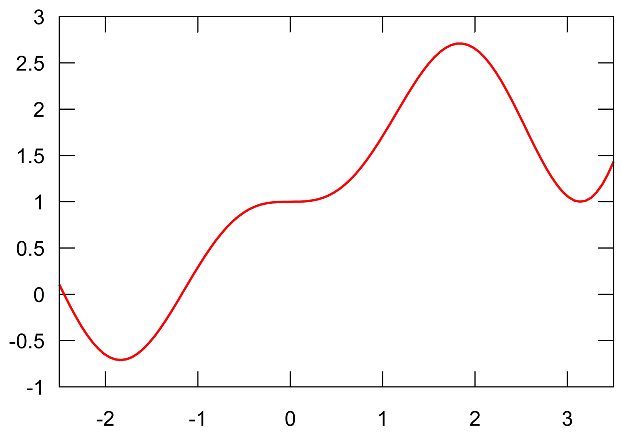

Figure 3.3 Plot of the function $f(x) = x\sin(x)^2 + 1$.

$$w_j = w_j - \alpha \frac{d}{dw_j} C(\mathbf{w}, b) \tag{3.11}$$

$$b = b - \alpha \frac{d}{db} C(\mathbf{w}, b) \tag{3.12}$$

Assuming a sufficient number of iterations, and a learning rate α that is not too large, $\mathbf{w}$ and b are guaranteed to converge to the optimal values because the logistic regression cost function is convex.[4] However, one problem with this approach is that computing the two partial derivatives requires the inspection of *all* training examples (this is what the summation in Equation 3.8 indicates), which means that the learning algorithm would have to do many passes over the training dataset before any meaningful changes are observed. Because of this, in practice, we do not compute C over the whole training data, but over a small number of examples at a time. This small group of examples is called a *mini batch*. In the simplest case, the size of the mini batch is 1, i.e., we update the $\mathbf{w}$ and b weights after seeing each individual example i, using a cost function computed for example i alone:

$$C_i(\mathbf{w}, b) = -(y_i \log \sigma(\mathbf{x}_i; \mathbf{w}, b) + (1 - y_i)\log(1 - \sigma(\mathbf{x}_i; \mathbf{w}, b))) \tag{3.13}$$

This simplified form of gradient descent is called *stochastic gradient descent* (SGD), where "stochastic" indicates that we work with a stochastic approximation (or an estimate) of C.

[4] Demonstrating that the LR cost function is convex is beyond the scope of this book. The interested reader may read other materials on this topic such as http://mathgotchas.blogspot.com/2011/10/why-is-error-function-minimized-in.html.

Algorithm 5: Logistic regression learning algorithm using stochastic gradient descent.

```
w = 0
b = 0
while not converged do
    for each training example $\mathbf{x}_i$ in X do
        for each $w_j$ in w do
            $w_j = w_j - \alpha \frac{d}{dw_j} C_i(\mathbf{w}, b)$
        end
        $b = b - \alpha \frac{d}{db} C_i(\mathbf{w}, b)$
    end
end
```

Building from the last three equations above, we can write the logistic regression training algorithm as shown in Algorithm 5. The reader will immediately see that this formulation of the algorithm is similar to Algorithm 4, which we introduced at the beginning of this chapter. In the next section, we will demonstrate that these two algorithms are indeed equivalent, by computing the two partial derivatives $\frac{d}{dw_j}C_i(\mathbf{w},b)$ and $\frac{d}{db}C_i(\mathbf{w},b)$.

3.4 Deriving the Logistic Regression Update Rule

Here we will compute the partial derivative of the cost function $C_i(\mathbf{w},b)$ of an individual example i, with respect to each feature weight w_j and bias term b. For these operations we will rely on several rules to compute the derivatives of a few necessary functions. These rules are listed in Table 3.1.

Let us start with the derivative of C with respect to one feature weight w_j:

$$\frac{d}{dw_j}C_i(\mathbf{w},b) = \frac{d}{dw_j}(-y_i \log \sigma(\mathbf{x}_i;\mathbf{w},b) - (1-y_i)\log(1-\sigma(\mathbf{x}_i;\mathbf{w},b)))$$

Let us use σ_i to denote $\sigma(\mathbf{x}_i;\mathbf{w},b)$ below, for simplicity:

$$= \frac{d}{dw_j}(-y_i \log \sigma_i - (1-y_i)\log(1-\sigma_i))$$

Pulling out the y_i constants and then applying the chain rule on the two logarithms:

$$= -y_i \frac{d}{d\sigma_i}\log \sigma_i \frac{d}{dw_j}\sigma_i - (1-y_i)\frac{d}{d(1-\sigma_i)}\log(1-\sigma_i)\frac{d}{dw_j}(1-\sigma_i)$$

After applying the derivative of the logarithm:

$$= -y_i \frac{1}{\sigma_i} \frac{d}{dw_j} \sigma_i - (1-y_i) \frac{1}{1-\sigma_i} \frac{d}{dw_j} (1-\sigma_i)$$

After applying the chain rule on $\frac{d}{dw_j}(1-\sigma_i)$:

$$\begin{aligned}
&= -y_i \frac{1}{\sigma_i} \frac{d}{dw_j} \sigma_i + (1-y_i) \frac{1}{1-\sigma_i} \frac{d}{dw_j} \sigma_i \\
&= (-y_i \frac{1}{\sigma_i} + (1-y_i) \frac{1}{1-\sigma_i}) \frac{d}{dw_j} \sigma_i \\
&= \frac{-y_i(1-\sigma_i) + (1-y_i)\sigma_i}{\sigma_i(1-\sigma_i)} \frac{d}{dw_j} \sigma_i \\
&= \frac{\sigma_i - y_i}{\sigma_i(1-\sigma_i)} \frac{d}{dw_j} \sigma_i
\end{aligned}$$

After applying the chain rule on σ_i:

$$= \frac{\sigma_i - y_i}{\sigma_i(1-\sigma_i)} \frac{d}{d(\mathbf{w} \cdot \mathbf{x}_i + b)} \sigma_i \frac{d}{dw_j} (\mathbf{w} \cdot \mathbf{x}_i + b)$$

After the derivative of the sigmoid and then canceling numerator and denominator:

$$\begin{aligned}
&= \frac{\sigma_i - y_i}{\sigma_i(1-\sigma_i)} \sigma_i(1-\sigma_i) \frac{d}{dw_j} (\mathbf{w} \cdot \mathbf{x}_i + b) \\
&= (\sigma_i - y_i) \frac{d}{dw_j} (\mathbf{w} \cdot \mathbf{x}_i + b)
\end{aligned}$$

Lastly, after applying the derivative of the dot product:

$$= (\sigma_i - y_i) x_{ij} \tag{3.14}$$

where x_{ij} is the value of feature j in the feature vector $\mathbf{x_i}$.

Following a similar process, we can compute the derivative of C_i with respect to the bias term as:

$$\frac{d}{db} C_i(\mathbf{w}, b) = \frac{d}{db} (-y_i \log \sigma(\mathbf{x}_i; \mathbf{w}, b) - (1-y_i) \log(1 - \sigma(\mathbf{x}_i; \mathbf{w}, b))) = \sigma_i - y_i \tag{3.15}$$

Knowing that σ_i is equivalent with decision($\mathbf{x}_i$, $\mathbf{w}$, b), one can immediately see that applying Equation 3.15 in line 8 of Algorithm 5 transforms the update of the bias into the form used in Algorithm 4 (line 7). Similarly, replacing the partial derivative in line 6 of Algorithm 5 with its explicit form from Equation 3.14 yields an update equivalent with the weight update used in Algorithm 4. The superficial difference between the two algorithms is that Algorithm 5 updates each feature weight w_j explicitly, whereas Algorithm 4 updates *all* weights at once by updating the entire vector $\mathbf{w}$. Needless to say, these two forms are equivalent. We prefer the

Table 3.1 Rules of computation for a few functions necessary to derive the logistic regression update rules. In these formulas, f and g are functions, a and b are constants, x is a variable.

Description	Formula
Chain rule	$\frac{d}{dx}f(g(x)) = \frac{d}{dg(x)}f(g(x))\frac{d}{dx}g(x)$
Derivative of summation	$\frac{d}{dx}(af(x)+bg(x))) = a\frac{d}{dx}f(x)+b\frac{d}{dx}g(x)$
Derivative of natural logarithm	$\frac{d}{dx}\log(x) = \frac{1}{x}$
Derivative of sigmoid	$\frac{d}{dx}\sigma(x) = \frac{d}{dx}(\frac{1}{1+e^{-x}}) = -\frac{1}{(1+e^{-x})^2}(-e^{-x}) = \sigma(x)(1-\sigma(x))$
Derivative of dot product between vectors $\mathbf{x}$ and $\mathbf{a}$ with respect to x_i	$\frac{d}{dx_i}(\mathbf{x}\cdot\mathbf{a}) = a_i$

explicit description in Algorithm 5 for clarity. But, in practice, one is more likely to implement Algorithm 4 because vector operations are efficiently implemented in most machine learning software libraries.

3.5 From Binary to Multiclass Classification

So far, we have discussed binary logistic regression, where we learned a classifier for two labels (1 and 0), where the probability of label 1 is computed as: $p(y=1|\mathbf{x};\mathbf{w},b) = \sigma(\mathbf{x};\mathbf{w},b)$ and probability of label 0 is: $p(y=0|\mathbf{x};\mathbf{w},b) = 1-p(y=1|\mathbf{x};\mathbf{w},b) = 1-\sigma(\mathbf{x};\mathbf{w},b)$. However, there are many text classification problems where two labels are not sufficient. For example, we might decide to implement a movie review classifier that produces five labels, to capture ratings on a five-star scale. To accommodate this class of problems, we need to generalize the binary LR algorithm to multiclass scenarios, where the labels to be learned may take values from 1 to k, where k is the number of classes to be learned, e.g., 5 in the previous example.

Figure 3.4 provides a graphical explanation of the multiclass LR. The key observation is that now, instead of maintaining a single weight vector $\mathbf{w}$ and bias b, we maintain one such vector and bias term *for each* class to be learned. This complicates our notations a bit: instead of using a single index to identify positions in an input vector $\mathbf{x}$ or in $\mathbf{w}$, we now have to maintain two. That is, we will use $\mathbf{w}_i$ to indicate the weight vector for class i, w_{ij} to point to the weight of the edge that connects the input x_j to the class i, and b_i to indicate the bias term for class i. The output of each "neuron" i in the figure produces a score for label i, defined as the sum between the bias term of class i and the dot product of the weight vector

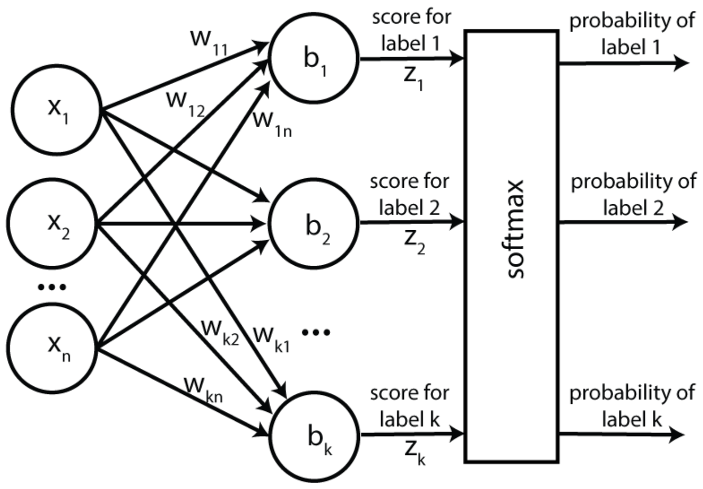

Figure 3.4 Multiclass logistic regression.

for class i and the input vector. More formally, if we use z_i to indicate the score for label i, then: $z_i = \mathbf{w}_i \cdot \mathbf{x} + b_i$.

Note that these scores are not probabilities: they are not bounded between 0 and 1, and they will not sum up to 1. To turn them into probabilities, we are introducing a new function, called softmax, which produces probability values for the k classes. For each class i, softmax defines the corresponding probability as:

$$p(y = i|\mathbf{x};\mathbf{W},\mathbf{b}) = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}} = \frac{e^{\mathbf{w}_i \cdot \mathbf{x} + b_i}}{\sum_{j=1}^{k} e^{\mathbf{w}_j \cdot \mathbf{x} + b_j}} \tag{3.16}$$

where the $\mathbf{W}$ matrix stores all $\mathbf{w}$ weight vectors, i.e., row i in $\mathbf{W}$ stores the weight vector $\mathbf{w}_i$ for class i, and the $\mathbf{b}$ vector stores all bias values, i.e., b_i is the bias term for class i.

Clearly, the softmax function produces probabilities: (a) the exponent function used guarantees that the softmax values are positives, and (b) the denominator, which sums over all the k classes guarantees that the resulting values are between 0 and 1, and sum up to 1. Further, with just a bit of math, we can show that the softmax for two classes reduces to the sigmoid function. Using the softmax formula, the probability of class 1 in a two-class LR (using labels 1 and 0) is:

$$\begin{aligned} p(y = 1|\mathbf{x};\mathbf{W},\mathbf{b}) &= \frac{e^{\mathbf{w}_1 \cdot \mathbf{x} + b_1}}{e^{\mathbf{w}_0 \cdot \mathbf{x} + b_0} + e^{\mathbf{w}_1 \cdot \mathbf{x} + b_1}} = \frac{1}{\frac{e^{\mathbf{w}_0 \cdot \mathbf{x} + b_0}}{e^{\mathbf{w}_1 \cdot \mathbf{x} + b_1}} + 1} \\ &= \frac{1}{e^{-((\mathbf{w}_1 - \mathbf{w}_0) \cdot \mathbf{x} + (b_1 - b_0))} + 1} \end{aligned} \tag{3.17}$$

Using a similar derivation, which we leave as an at-home exercise to the curious reader, the probability of class 0 is:

$$\begin{aligned} p(y=0|\mathbf{x};\mathbf{W},\mathbf{b}) &= \frac{e^{\mathbf{w}_0\cdot\mathbf{x}+b_0}}{e^{\mathbf{w}_0\cdot\mathbf{x}+b_0}+e^{\mathbf{w}_1\cdot\mathbf{x}+b_1}} = \frac{e^{-((\mathbf{w}_1-\mathbf{w}_0)\cdot\mathbf{x}+(b_1-b_0))}}{e^{-((\mathbf{w}_1-\mathbf{w}_0)\cdot\mathbf{x}+(b_1-b_0))}+1} \\ &= 1-p(y=1|\mathbf{x};\mathbf{W},\mathbf{b}) \end{aligned} \tag{3.18}$$

From these two equations, we can immediately see that two the formulations of binary LR, i.e., sigmoid vs. softmax, are equivalent when we set the parameters of the sigmoid to be equal to the the difference between the parameters of class 1 and the parameters of class 0 in the softmax formulation, or $\mathbf{w} = \mathbf{w}_1 - \mathbf{w}_0$, and $b = b_1 - b_0$, where $\mathbf{w}$ and b are the sigmoid parameters in Equations 3.2 and 3.3.

The cost function for multiclass LR follows the same intuition and formalization as the one for binary LR. That is, during training we want to maximize the probabilities of the correct labels assigned to training examples, or, equivalently, we want to minimize the negative log likelihood of the data. Similarly to Equation 3.7, the cost function for multiclass LR is defined as:

$$C(\mathbf{W},\mathbf{b}) = -\log L(\mathbf{W},\mathbf{b}) = -\sum_{i=1}^{m} \log p(y=y_i|\mathbf{x}_i;\mathbf{W},\mathbf{b}) \tag{3.19}$$

or, for a single training example i:

$$C_i(\mathbf{W},\mathbf{b}) = -\log p(y=y_i|\mathbf{x}_i;\mathbf{W},\mathbf{b}) \tag{3.20}$$

where y_i is the correct label for training example i, and $\mathbf{x}_i$ is the feature vector for the same example. The probabilities in this cost function are computed using the softmax formula, as in Equation 3.16. This cost function, which generalizes the negative log likelihood cost function to multiclass classification, is called *cross entropy*. This is probably the most commonly used cost function in NLP problems. We will see it a lot throughout the book.

The learning algorithm for multiclass LR stays almost the same as Algorithm 5, with small changes to account for the different cost function and the larger number of parameters, i.e., we now update a matrix $\mathbf{W}$ instead of a single vector $\mathbf{w}$, and a vector $\mathbf{b}$ instead of the scalar b. The adjusted algorithm is shown in Algorithm 6. We leave the computation of the derivatives used in Algorithm 6 as an at-home exercise for the interested reader. However, as we will see in the next chapter, we can now rely on automatic differentiation libraries such as PyTorch to compute these derivatives for us, so this exercise is not strictly needed to implement multiclass LR.

3.6 Evaluation Measures for Multiclass Text Classification

Now that we generalized our classifier to operate over an arbitrary number of classes, it is time to generalize the evaluation measures introduced in Section 2.3 to multiclass problems as well.

Algorithm 6: Learning algorithm for multiclass logistic regression.

```
1  W = 0
2  b = 0
3  while not converged do
4      for each training example $\mathbf{x}_i$ in X do
5          for each $w_{jk}$ in W do
6              $w_{jk} = w_{jk} - \alpha \frac{d}{dw_{jk}} C_i(\mathbf{W}, \mathbf{b})$
7          end
8          for each $b_j$ in b do
9              $b_j = b_j - \alpha \frac{d}{db_j} C_i(\mathbf{W}, \mathbf{b})$
10         end
11     end
12 end
```

Table 3.2 Example of a confusion matrix for three-class classification. The dataset contains 1,000 data points, with 1 data point in class $C1$, 100 in class $C2$, and 899 in class $C3$.

	Classifier predicted $C1$	Classifier predicted $C2$	Classifier predicted $C3$
Gold label is $C1$	1	1	0
Gold label is $C2$	10	80	10
Gold label is $C3$	1	8	890

Throughout this section, we will use as a walkthrough example a three-class version of the Medicaid application classification problem from Section 2.3. In this version, our classifier has to assign each application to one of three classes, where classes $C1$ and $C2$ indicate the high- and medium-priority applications, and class $C3$ indicate regular applications that do not need to be rushed through the system. Same as before, most applications fall under class $C3$. Table 3.2 shows an example confusion matrix for this problem for a hypothetical three-class classifier that operates over an evaluation dataset that contains 1,000 applications.

The definition of accuracy remains essentially the same for multiclass classification, i.e., accuracy is the ratio of data points classified correctly. In general, the number of correctly classified points can be computed by summing up the counts on the diagonal of the confusion matrix. For example, for the confusion matrix shown in Table 3.2, accuracy is $\frac{1+80+890}{1{,}000} = \frac{971}{1{,}000}$.

Similarly, the definitions of precision and recall for an individual class c, remain the same:

$$P_c = \frac{TP_c}{TP_c + FP_c} \tag{3.21}$$

$$R_c = \frac{TP_c}{TP_c + FN_c} \tag{3.22}$$

where TP_c indicate the number of true positives for class c, FP_c indicate the number of positives for class c, and FN_c indicate the number of false negatives for the same class. However, because we now have more than two rows and two columns in the confusion matrix, we have to do a bit more additional math to compute the FP_c and FN_c counts. In general, the number of false positives for a class c is equal to the sum of the counts in the column corresponding to class c, excluding the element on the diagonal. The number of of false negatives for a class c is equal to the sum of the counts in the corresponding row, excluding the element on the diagonal. For example, for class $C2$ in the table, the number of true positives is $TP_{C2} = 80$, the number of false positives is $FP_{C2} = 1 + 8 = 9$, and the number of false negatives is $FN_{C2} = 10 + 10 = 20$. Thus, the precision and recall for class $C2$ are: $P_{C2} = \frac{80}{80+9} = 0.90$, and $R_{C2} = \frac{80}{80+20} = 0.80$. We leave it as an at-home exercise to show that $P_{C1} = 0.08$, $R_{C1} = 0.5$, $P_{C3} = 0.99$, and $R_{C3} = 0.99$. From these values, one can trivially compute the respective F scores per class.

The important discussion for multiclass classification is how to average these sets of precision/recall scores into single values that will give us a quick understanding of the classifier's performance? There are two strategies to this end, both with advantages and disadvantages:

Macro averaging: Under this strategy we simply average all the individual precision/recall scores into a single value. For example, for the above example, the macro precision score over all three classes is: macro $P = \frac{P_{C1}+P_{C2}+P_{C3}}{3} = \frac{0.08+0.90+0.99}{3} = 0.66$. Similarly, the macro recall score is: macro $R = \frac{R_{C1}+R_{C2}+R_{C3}}{3} = \frac{0.50+0.80+0.99}{3} = 0.76$. The macro F_1 score is the harmonic mean of the macro precision and recall scores.

As discussed in Section 2.3, in many NLP tasks the labels are highly unbalanced, and we commonly care less about the most frequent label. For example, here we may want to measure the performance of our classifier on classes $C1$ and $C2$, which require rushed processing in the Medicaid system. In such scenarios, the macro precision and recall scores exclude the frequent class, e.g., $C3$ in our case. Thus, the macro precision becomes: macro $P = \frac{P_{C1}+P_{C2}}{2} = \frac{0.08+0.90}{2} = 0.49$, which is more indicative of the fact that our classifier does not perform too well on the two important classes in this example.

The advantage of the macro scores is that they treat all the classes we are interested in as equal contributors to the overall score. But, depending on the task, this may also be a disadvantage. For example, in the above example, the latter macro precision score of 0.49

hides the fact that our classifier performs reasonably well on the $C2$ class ($P_{C2} = 0.90$), which is 100 times more frequent than $C1$ in the data!

Micro averaging: This strategy addresses the above disadvantage of macro averaging, by computing overall precision, recall, and F scores where each class contributes proportionally with its frequency in the data. In particular, rather than averaging the individual precision/recall scores, we compute them using the class counts directly. For example, the micro precision and recall scores for the two classes of interest in the above example, $C1$ and $C2$, are:

$$\text{micro } P = \frac{TP_{C1} + TP_{C2}}{TP_{C1} + TP_{C2} + FP_{C1} + FP_{C2}} = \frac{1+80}{1+80+11+9} = 0.80 \tag{3.23}$$

$$\text{micro } R = \frac{TP_{C1} + TP_{C2}}{TP_{C1} + TP_{C2} + FN_{C1} + FN_{C2}} = \frac{1+80}{1+80+1+20} = 0.79 \tag{3.24}$$

Similar to macro averaging, the micro F_1 score is computed as the harmonic mean of the micro precision and recall scores.

Note that in this example, the micro scores are considerably higher than the corresponding macro scores because: (a) the classifier's performance on the more frequent $C2$ class is higher than the performance on class $C1$, and (b) micro averaging assigns more importance to the frequent classes, which, in this case, raises the micro precision and recall scores. The decision of which averaging strategy to use is problem specific, and depends on the answer to the question: should all classes be treated equally during scoring, or should they be weighted by their frequency in the data? In the former case, the appropriate averaging is macro; in the latter, micro.

3.7 Drawbacks of Logistic Regression

The logistic regression algorithm solves the lack of smooth updates in the Perceptron algorithm through its improved update functions on its parameters. This seemingly small change has an important practical impact: in most NLP applications, logistic regression tends to outperform the Perceptron.

However, the other drawbacks observed with the Perceptron still hold. Binary logistic regression is also a linear classifier because its decision boundary remains a hyperplane. It is tempting to say that the above statement is not correct because the sigmoid is clearly a nonlinear function. However, the linearity of the binary LR classifier is easy to prove with just a bit of math. Remember that the decision function for the binary LR is: if $\frac{1}{1+e^{-(\mathbf{w}\cdot\mathbf{x}+b)}} \geq 0.5$ we assign one label, and if $\frac{1}{1+e^{-(\mathbf{w}\cdot\mathbf{x}+b)}} < 0.5$ we assign the other label. Thus, the decision boundary is defined by the equation $\frac{1}{1+e^{-(\mathbf{w}\cdot\mathbf{x}+b)}} = 0.5$. From this we can easily derive that $e^{-(\mathbf{w}\cdot\mathbf{x}+b)} = 1$, and $-(\mathbf{w}\cdot\mathbf{x}+b) = 0$, where the latter is a linear function on the parameters $\mathbf{w}$ and b. This observation generalizes to the multiclass logistic regression introduced in Section 3.5. In the multiclass scenario, the decision boundary between all classes consists of multiple intersecting

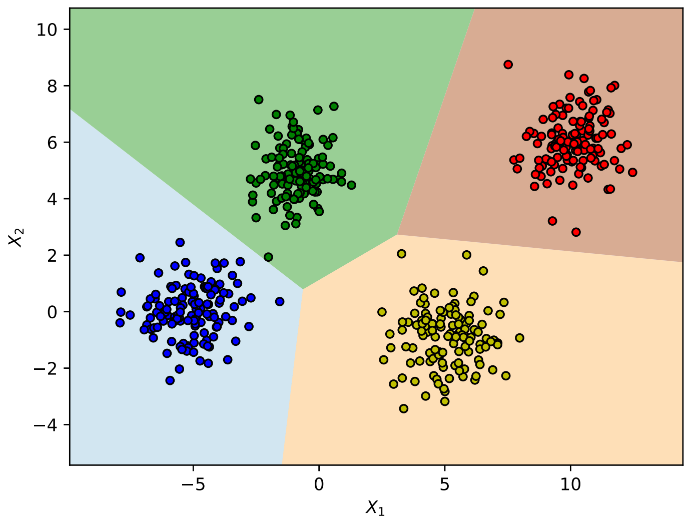

Figure 3.5 Example of a two-dimensional decision boundary for a 4-class logistic regression classifier. This figure was generated by Clayton Morrison and is reproduced with permission.

segments, each of which are fragments of a hyperplane. Figure 3.5 shows an example of such a decision boundary for a 4-class problem, where each data point is described by two features: x_1 and x_2. Clearly, forcing these segments to be linear reduces what the multiclass logistic regression can learn.

Further, similar to the Perceptron, the LR covered so far relies on hand-crafted features, which, as discussed in the previous chapter, may be cumbersome to generate and may generalize poorly. Lastly, logistic regression also focuses on individual predictions rather than structured learning. We will address all these limitations in the following chapters. We will start by introducing non-linear classifiers in Chapter 5.

3.8 Historical Background

TODO: To do

3.9 References and Further Readings

TODO: To do

4 Implementing a Review Classifier Using Logistic Regression in PyTorch

In the previous chapters we have discussed the theory behind Perceptrons and logistic regression, including mathematical explanations of how and why they are able to learn from examples. In this chapter we will transition from math to code. Specifically, we will discuss how to implement these models in the Python programming language.

As the book progresses, we will introduce popular tools and libraries that make Python the language of choice for machine learning (e.g., PyTorch,[1], Hugging Face's transformers,[2] among others.) However, to get a better understanding of how these algorithms work under the hood, we will start by implementing them from scratch. Afterwards, we will transition to an implementation that relies on PyTorch.

To make things as concrete as possible, this chapter starts with a description of the review classification dataset that we will use as our running example. In the same section, we will implement the code necessary to load this dataset. Then we will implement the algorithms discussed in the previous chapters and we will evaluate them on this dataset.

TODO: paragraph mentioning the repo, and how it's organized. And that we start with a small overview of the Python language in the next section.

4.1 Overview of the Python Programming Language

TODO: todo at the end. Mention that it is not comprehensive, but instead focuses on the features relevant to NLP and ML. Include subsections on NumPy and PyTorch. Maybe separate in two sections: first vanilla Python, and a separate section on NumPy and PyTorch?

4.2 Large Movie Review Dataset

In the first part of this chapter, we will focus on binary classification. That is, we aim to train classifiers that assign one of two labels to a given text. In particular, we will use the Large Movie Review Dataset [**?**][3] as the example dataset for this task. This contains movie reviews

[1] https://pytorch.org

[2] https://huggingface.co

[3] https://ai.stanford.edu/~amaas/data/sentiment/

and their associated scores (between 1 and 10) as provided by people on the IMDb website.[4] We will convert these scores to binary labels by assigning a positive review label to scores above 6, and a negative label to scores below 5. Reviews with scores 5 and 6 are considered too neutral and are not included as part of the labeled examples.

The dataset is divided in two even partitions called *train* and *test*, each containing 25,000 reviews. The dataset also provides additional unlabeled reviews, but we will not use those. Each partition contains two directories called `pos` and `neg` where the positive and negative examples are stored. Each review is stored in an independent text file, whose name is composed of an id unique to the partition and the score associated to the review, separated by an underscore. An example of a positive and a negative review is shown in Table 4.2.

Filename	Score	Review Text
`train/pos/24_8.txt`	8/10	*Although this was obviously a low-budget production, the performances and the songs in this movie are worth seeing. One of Walken's few musical roles to date. (he is a marvelous dancer and singer and he demonstrates his acrobatic skills as well - watch for the cartwheel!) Also starring Jason Connery. A great children's story and very likable characters.*
`train/neg/141_3.txt`	3/10	*This stalk and slash turkey manages to bring nothing new to an increasingly stale genre. A masked killer stalks young, pert girls and slaughters them in a variety of gruesome ways, none of which are particularly inventive. It's not scary, it's not clever, and it's not funny. So what was the point of it?*

Table 4.1 Two examples of movie reviews from IMDb. The first one is a positive review of the movie *Puss in Boots (1988)*. The second one is a negative review of the movie *Valentine (2001)*. Both reviews can be found at https://www.imdb.com/review/rw0606396/ and https://www.imdb.com/review/rw0721861/, respectively.

4.2.1 Preparing the Dataset

Before we start implementing our classifier, it is important that we prepare the data, i.e., the free text associated with the reviews we will analyze, into a more structured format that is more suited for machine learning. Specifically, we will: (a) normalize and break the text into words, (b) assign a unique identifier (id) to each unique word, and, lastly, (c) construct a feature vector for each review. These are practical concerns that need to be addressed before

[4] https://www.imdb.com/

we get to more exciting part of actually training a classifier. If you are eager to see the implementation of the classifier then you can skip this section. However, we recommend you come back and read about these steps, since you probably will need to go through a similar process over your own data once you start applying the techniques learned in this book.

4.2.1.1 Text Normalization

Text normalization is the process of transforming text into a canonical form, so that we operate over it consistently and robustly. The dataset we are working with consists of movie reviews written in English. However, we should not make any assumptions about the underlying texts, as they are reviews written by many different people and found "in the wild." Therefore, we will probably find reviews that include extraneous characters that are essentially noise and not useful for classification. Some of these characters may not even be visible, as they can be control characters not meant to be seen by humans, so just opening the reviews and taking a glimpse may not be sufficient to detect their presence. The first step of normalization addresses these extraneous characters.

There are two main ways in which computers encode text. The first is the American Standard Code for Information Interchange (ASCII), which encodes 128 characters, including letters, digits, punctuation, and some (invisible) control characters. This is sufficient for most English text. However, since the advent of the Internet, better ways for encoding text had to be devised in order to handle the multiple alphabets and languages. This was the motivation for the development of the Unicode standard, which supports considerable more characters than ASCII.[5] For consistency and to get rid of extraneous non-ASCII characters, in this chapter we will convert all texts in our dataset to ASCII. However, please note that this step cannot be used for languages that use widely different alphabets than English, e.g., Arabic or Chinese.

Second, in our current application we want to compare words in a case-insensitive manner. While case information has clear meaning in English (e.g., "may" is different than "May"), online, informal text commonly omits case information. Thus, it is more robust to simply remove case information from all words. Removing case may seem trivial in English: just turn everything to lowercase. However, things get more complicated when we need to consider international writing systems. For this purpose, the Unicode standard defines a casefolding procedure that is more aggressive than just converting to lowercase, and can be used for comparing strings while disregarding case differences. Python supports this through the `casefold()` string method.

An implementation of our text normalization procedure is shown in Figure 4.1. Note that, as discussed, this text normalization is not universal, and you may have to modify it according to your own needs. For example, discarding all non-ASCII characters may be too aggressive for your application.

[5] For example, Unicode 13.0 supports 143,859 characters.

```python
def normalize_text(text):
    # convert all text to lowercase, aggressively
    text = text.casefold()
    # discard any non-ascii character
    text = text.encode('ascii', 'ignore').decode('ascii')
    # return normalized text
    return text
```

Figure 4.1 Text normalization procedure that uses Unicode casefolding and discards all non-ASCII characters.

4.2.1.2 Tokenization

As discussed in Chapter 2.2, we will generate features for our classifier using a simple, bag-of-words approach, in which each word is a distinct feature and its value is the number of times that particular word appears in the review. To achieve this, we first need to *tokenize* the text, i.e., break it into individual pieces called *tokens*. In general, a token is a "instance of a sequence of characters that are grouped together as a useful semantic unit for processing" [**?**]. Intuitively, this usually corresponds to words in natural language. Further, we define a *term* as a unique token, possibly normalized in some way. For example, in the text *To be or not to be*, there are six tokens, and four terms (assuming that normalization converts the tokens to lower case): *to*, *be*, *or*, and *not*.

Tokenization sounds simple, but in practice it is a tricky process that requires many, possibly arbitrary decision, e.g. should phone numbers be a single token or several?, should we tokenize around hyphens?, etc. In this book, we will rely on existing tools for English tokenization. In particular, we will use NLTK's `sent_tokenize()` to break a text into individual sentences, and, more importantly, on the `TweetTokenizer` class for actual tokenization. This tokenizer was designed for the tokenization of social media texts, and, thus, it is better suited for the tokenization of our reviews.

The function to tokenize movie reviews is shown in Figure 4.2. Note that we only include "valid" tokens in the results (lines 30 and 31). The `is_valid()` function, which evaluates if a token is valid, arbitrarily discards tokens that we decided are not important for classification such as numbers and non-letter symbols.

4.2.1.3 Vocabulary

We previously mentioned that we need to assign a unique id to each unique token, or term. For this purpose, we will write a `Vocabulary` class that keeps track of this mapping. We will also add a special term called `[UNK]` that we will use to represent terms that are unknown to this vocabulary (so we can manage new words that appear during evalua-

```python
import string
from nltk.tokenize import sent_tokenize
from nltk.tokenize.casual import TweetTokenizer

def is_valid(token):
    """returns True if `token` is a valid token"""
    invalid = string.punctuation + string.whitespace
    if any(c.isdigit() for c in token):
        # reject any token that contains at least one digit
        return False
    elif all(c in invalid for c in token):
        # reject tokens composed of invalid characters only,
        # except the question and exclamation marks
        return token in ('?', '!')
    else:
        # accept everything else
        return True

def tokenize(text):
    """gets a string and returns a list of tokens"""
    tokens = []
    # we use TweetTokenizer because it is suitable for social media posts
    tokenizer = TweetTokenizer(reduce_len=True)
    for sent in sent_tokenize(text):
        # we help the tokenizer a little bit by adding spaces
        # around dots and double dashes
        sent = sent.replace('.', ' . ').replace('--', ' -- ')
        for token in tokenizer.tokenize(sent):
            # only add valid tokens to the vocabulary
            if is_valid(token):
                tokens.append(token)
    return tokens

def tokenize_imdb_review(filename):
    """returns the tokenized contents of a file"""
    with open(filename) as f:
        text = normalize_text(f.read())
    # remove html line breaks
    text = text.replace('<br />', ' ')
    return tokenize(text)
```

Figure 4.2 Text tokenization procedure that uses NLTK's `sent_tokenize` as well as `TweetTokenizer` to tokenize the movie reviews.

tion).[6] Specifically, when the `get_token_id(token)` method is called with a token that has never been encountered before, the id of `[UNK]` will be returned. The method called `add_token(token)` similarly returns the id of the provided token, with the exception that new tokens are added to the vocabulary. This latter method will be used during training, when the vocabulary will be built on the fly. The complementary method `get_token(id)` receives an id and returns the corresponding term if the id is valid, or `[UNK]` otherwise. The

[6] `[UNK]` is not the only special token that is commonly used by NLP models. We will add more in subsequent chapters.

size of the vocabulary can be retrieved by calling `len(vocabulary)`. The Python code for the `Vocabulary` class is shown in Figure 4.3.

4.2.1.4 Reading the Dataset

Now we have all the pieces necessary to read the dataset. The `read_imdb_data` function shown in Figure 4.4 aggregates all these components into code that reads the review dataset. The function takes as arguments the path to the directory where the data is stored, the vocabulary that stores all encountered terms, and a Boolean parameter that indicates if we need to add terms to the vocabulary (during training), or not (during evaluation). The function assumes that the provided directory contains two other subdirectories called `pos` and `neg`, which contain the text files with the positive and negative reviews, respectively.

The final piece of the puzzle is the function shown in Figure 4.5, which takes as arguments the dataset produced by the `read_imdb_data` function, and encodes it as a matrix, or a two-dimensional NumPy array **X**. In this matrix, each row represents a review and each column represents a term in the vocabulary. Each x_{ij} cell in the matrix represents the number of times that term with id j appears in review i. We store the cells in **X** as the type `int32` to save space when storing the arrays to disk (as compared to 64-bit numbers). The function also encodes the labels assigned to reviews as a NumPy array, where each element is a Boolean value that indicates if the corresponding review is positive or not.

4.3 Perceptron

Now that we have defined our task and we know more about the corresponding dataset, we will proceed to implement a Perceptron classifier that can classify these movie reviews as positive or negative.

Although we will rely on the PyTorch deep learning library to implement our algorithms throughout most of this book, we would like the reader to have an understanding of the key concepts discussed, which are independent of a specific library. For this reason, we will start with a from scratch implementation of the binary Perceptron. In the next sections we will transition to PyTorch, and we will use this transition to highlight the key features of the library.

The code that implements Algorithm 2 is shown in Figure 4.6. Before any learning happens, this code loads the training dataset and generates the matrix **X** of training data points, and the vector of corresponding labels **y**. This happens in line 2 through the `read_data()` function. TODO: make this function name consistent: either read_data or read_imdb_data As discussed, the first object returned by the function is the two-dimensional NumPy array **X**, where each row is a datapoint from our dataset (i.e., a movie review) and columns represent the features used to represent the data point, i.e., counts of terms in this review. The second object is the one-dimensional array **y**, whose length is equal to the number of rows in the X matrix. Each element in **y** is a number that indicates if the corresponding row in **X** is a positive

```python
class Vocabulary:

    def __init__(self, i2t=None):
        self.i2t = [] if i2t is None else i2t
        # make mapping token->id by flipping id->token
        self.t2i = {t:i for i,t in enumerate(self.i2t)}
        # add special tokens
        self.unk_token = '[UNK]'
        self.unk_id = self.add_token(self.unk_token)

    def __len__(self):
        return len(self.i2t)

    @classmethod
    def load(cls, filename):
        """loads a vocabulary stored in a file"""
        with open(filename) as f:
            return cls(f.read().splitlines())

    def save(self, filename):
        """saves the vocabulary to a file"""
        with open(filename, 'w') as f:
            for t in self.i2t:
                print(t, file=f)

    def add_tokens(self, tokens):
        """adds a list of tokens to the vocabulary,
        and returns a list of token ids"""
        return [self.add_token(t) for t in tokens]

    def get_tokens(self, ids):
        """gets a list of ids and returns a list of tokens"""
        return [self.get_token(i) for i in ids]

    def get_token_ids(self, tokens):
        """gets a list of tokens and returns a list of token ids"""
        return [self.get_token_id(t) for t in tokens]

    def add_token(self, t):
        """adds a token to the vocabulary if it isn't already there,
        and returns the token id"""
        if t in self.t2i:
            i = self.t2i[t]
        else:
            i = len(self.i2t)
            self.i2t.append(t)
            self.t2i[t] = i
        return i

    def get_token(self, i):
        """returns the token corresponding to the provided id
        if there is one, otherwise it returns the [UNK] token"""
        if 0 <= i < len(self.i2t):
            return self.i2t[i]
        return self.unk_token

    def get_token_id(self, t):
        """returns the token id for the corresponding token,
        or the [UNK] token id if the word is not in the vocabulary"""
        return self.t2i.get(t, self.unk_id)
```

Figure 4.3 Vocabulary class used to keep track of the mapping between unique tokens (or terms) and their corresponding ids.

```python
from pathlib import Path

def read_imdb_data(data_dir: Path, vocabulary: Vocabulary, add_tokens: bool):
    all_token_ids, all_labels = [], []
    for fold in ['pos', 'neg']:
        d = data_dir/fold
        for f in d.glob('*.txt'):
            tokens = tokenize_imdb_review(f)
            if add_tokens:
                token_ids = vocabulary.add_tokens(tokens)
            else:
                token_ids = vocabulary.get_token_ids(tokens)
            # collect token_ids
            all_token_ids.append(token_ids)
            # collect corresponding label (fold name)
            all_labels.append(split)
    return all_token_ids, all_labels
```

Figure 4.4 The `read_imdb_data` function, which reads a corpus of IMDB reviews.

```python
import numpy as np

def to_numpy(all_token_ids, all_labels, vocabulary):
    n_rows = len(all_token_ids)
    n_cols = len(vocabulary)
    X = np.zeros((n_rows, n_cols), dtype=np.int32)
    y = np.zeros(n_rows, dtype=np.bool)
    for i in range(n_rows):
        y[i] = all_labels[i] == 'pos'
        token_ids = all_token_ids[i]
        for j in token_ids:
            X[i, j] += 1
    return X, y
```

Figure 4.5 The `to_numpy` function.

or a negative review (using 1 for positive and 0 for negative). TODO: you are using integers here for y, but in the previous section you said they are Boolean

Having read the data, we now need to initialize the Perceptron model to the right size, so that we can use it with the data we just loaded. Recall from Section 2.4 that a Perceptron is composed of a weight vector $\mathbf{w}$ and a bias term b. The size of $\mathbf{w}$ should correspond to the number of features in our dataset, i.e., the number of columns in $\mathbf{X}$, so we need to figure out what that number is. Fortunately, NumPy arrays have an attribute called `shape` that contains the array dimensions. We use this attribute in line 5 to figure out the number of examples and the number of features in our data. Then, we use this information in line 6 to initialize $\mathbf{w}$ with the correct number of zeros. In line 7 we initialize the scalar b with a single zero.

```
 1 # load dataset
 2 X, y = read_data("aclImdb/train")
 3 
 4 # init model
 5 n_examples, n_features = X.shape
 6 w = np.zeros(n_features)
 7 b = 0
 8 n_epochs = 10
 9 
10 print("training ...")
11 indices = list(range(n_examples))
12 for epoch in range(10):
13     print("epoch", epoch)
14     n_errors = 0
15     random.shuffle(indices)
16     for i in indices:
17         x = X[i]
18   y_true = y[i]
19   score = x @ w + b
20   y_pred = 1 if score > 0 else 0
21   if y_true == y_pred:
22       continue
23   elif y_true == 1 and y_pred == 0:
24       w = w + x
25       b = b + 1
26       n_errors += 1
27   elif y_true == 0 and y_pred == 1:
28       w = w - x
29       b = b - 1
30       n_errors += 1
31     if n_errors == 0:
32         break
```

Figure 4.6 From scratch implementation of the binary Perceptron learning algorithm.

Line 3 of Algorithm 2 indicates that we need to repeat the training loop until convergence. In this implementation, we will define convergence as predicting all examples correctly. This is very ambitious and not always possible, so we will also include a maximum number of epochs. That is, the training procedure stops if any of the following two conditions is true: we reached the maximum number of epochs (line 12), or we converged (lines 31–32).

A second crucial difference between our implementation here and the theoretical Algorithm 2, is that we randomize the order in which the training examples are seen at the beginning of each epoch. TODO: why; because otherwise we introduce random biases due to the order of the data points. An example would be nice. We accomplish this by storing the indices corresponding to the $\mathbf{X}$ matrix rows in a Python list (as seen in line 11), and then shuffling these indices at the beginning of each epoch (line 15).

Lines 16 to 30 align closely with Algorithm 2. We start by iterating over each example in our training data, storing the current example in the variable `x`, and its corresponding label in the variable `y_true`. Lines 19 and 20 correspond to the Perceptron decision function shown in Algorithm 1. Note that NumPy (as well as PyTorch) uses Python's `@` operator to indicate dot product between two arrays. We use it in line 19 to calculate the dot product of the example `x` and the weights `w` (plus the bias `b`) to obtain the predicted score. Then, we use this score in line 20 to decide if the predicted label is positive or negative.

If the prediction is correct (line 21) then no update is needed, and we can move on to the next training example. However, if the prediction is incorrect then we need to adjust `w` and `b`. We also count how many examples were incorrectly classified in the current epoch. This count is used in line 31 to decide if the model has converged, and if so, stop training.

TODO: Add evaluation code

5 Feed Forward Neural Networks

So far we have explored classifiers with decision boundaries that are linear, or, in the case of the multiclass logistic regression, a combination of linear segments. In this chapter, we will expand what we have learned so far to classifiers that are capable of learning non-linear decision boundaries. The classifiers that we will discuss here are called *feed forward neural networks*, and are a generalization of both logistic regression and the Perceptron. Without going into the theory behind it, it has been shown that, under certain conditions, these classifiers can approximate any function [**??**]. That is, they can learn decision boundaries of any arbitrary shape. Figure 5.1 shows a very simple example of a hypothetical situation where a non-linear decision boundary is needed for a binary classifier.

The good news is that we have already introduced the building blocks of feed forward neural networks (FFNN): the individual neuron, and the stochastic gradient learning algorithm. In this chapter, we are simply combining these building blocks in slightly more complicated ways, but without changing any of the fundamental operating principles.

5.1 Architecture of Feed Forward Neural Networks

Figure 5.2 shows the general architecture of FFNNs. As seen in the figure, FFNNs combine multiple layers of individual neurons, where each neuron in a layer l is fully connected to all neurons in the next layer, $l+1$. Because of this, architectures such as the one in the figure are often referred to as *fully-connected FFNNs*. This is not the only possible architecture for FFNNs: any arbitrary connections between neurons are possible. However, because fully-connected networks are the most common FFNN architecture seen in NLP, we will focus on these in this chapter, and omit the fully-connected modifier from now on, for simplicity.

Figure 5.2 shows that the neuron layers in a FFNN are grouped into three categories. These are worth explaining in detail:

Input layer: Similar to the Perceptron or logistic regression, the input layer contains a vector $\mathbf{x}$ that describes one individual data point. For example, for the review classification task, the input layer will be populated with features extracted from an individual review such as the presence (or count) of individual words. In Chapter 8 we will switch from such hand-crafted features to numerical representations of text that capture some of the underlying semantics of language, and thus, are better for learning. Importantly, the neural network is agnostic to the

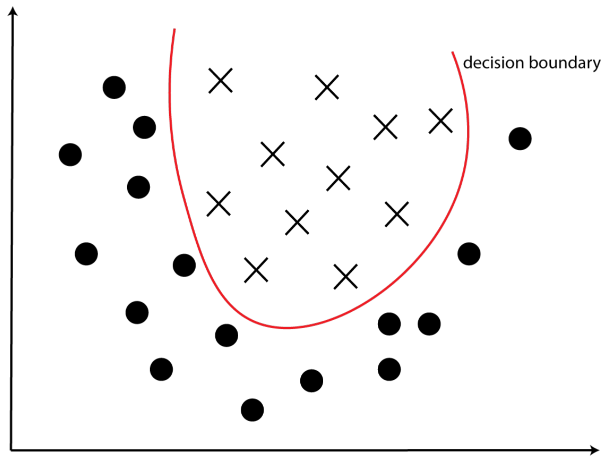

Figure 5.1 Decision boundary of a non-linear classifier.

way the representation of an input data point is created. All that matters for now is that each input data point is summarized with a vector of real values, $\mathbf{x}$.

Intermediate layers: Unlike the Perceptron and logistic regression, FFNNs have an arbitrary number of intermediate layers. Each neuron in an intermediate layer receives as inputs the outputs of the neurons in the previous layer, and produces an output (or activation) that is sent to all the neurons in the following layer. The activation of each neuron is constructed similarly to logistic regression, as a non-linear function that operates on the dot product of weights and inputs plus the bias term. More formally, the activation a_i^l of neuron i in layer l is calculated as:

$$a_i^l = f(\sum_{j=1}^{k} w_{ij}^l a_j^{l-1} + b_i^l) = f(\mathbf{w}_i^l \cdot \mathbf{a}^{l-1} + b_i^l) = f(z_i^l) \tag{5.1}$$

where k is the total number of neurons in the previous layer $l-1$, w_{ij}^l are the weights learned by the current neuron (neuron i in layer l), a_j^{l-1} is the activation of neuron j in the previous layer, and b_i^l is the bias term of the current neuron. For simplicity, we group all the weights w_{ij}^l into the vector $\mathbf{w}_i^l$, and all activations a_j^{l-1} into the vector $\mathbf{a}^{l-1}$. Thus, the summation in the equation reduces to the dot product between the two vectors: $\mathbf{w}_i^l \cdot \mathbf{a}^{l-1}$. We further denote the sum between this dot product and the bias term b_i^l as z_i^l. Thus, z_i^l is the output of neuron i in layer l right before the activation function f is applied.

The function f is a non-linear function that takes z_i^l as its input. For example, for the logistic regression neuron, f is the sigmoid function, σ. Many other non-linear functions are possible and commonly used in neural networks. We will discuss several such functions, together with

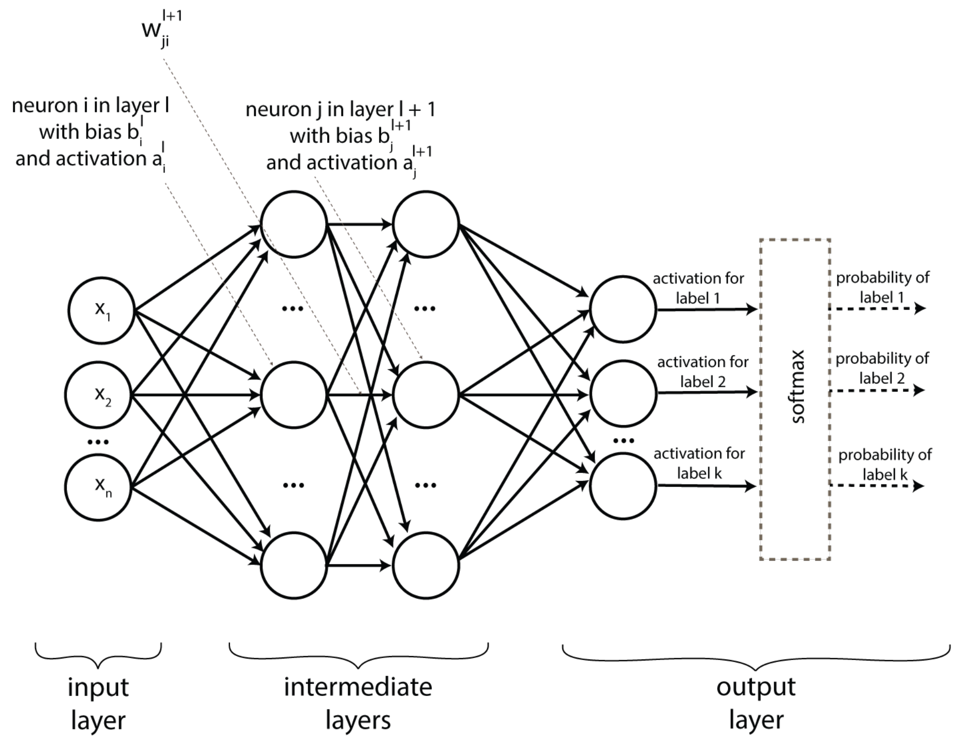

Figure 5.2 Fully-connected feed-forward neural network architecture.

their advantages and disadvantages in Chapter 6. What is important to realize at this stage is that these non-linear functions are what give neural networks the capability of learning non-linear decision boundaries. A multi-layer FFNN with linear activation functions remains a linear classifier. As a simple example, consider the neural network in Figure 5.3, which has one intermediate layer with two neurons, and a single neuron in the output layer. Let us consider that the activation function in each neuron is a "pass through" linear function $f(x) = x$. The activation of the output neuron is then computed as:

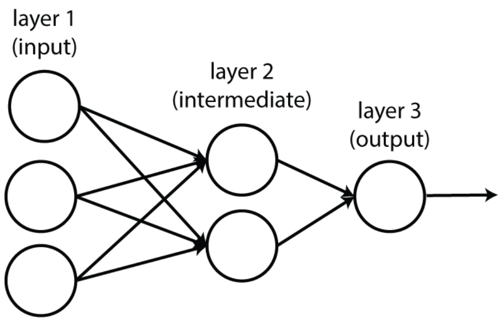

Figure 5.3 A feed-forward neural network with linear activation functions is a linear classifier.

$$\begin{aligned}
a_1^3 &= w_{11}^2 a_1^2 + w_{12}^2 a_2^2 + b_1^3 \\
&= w_{11}^2 (w_{11}^1 x_1 + w_{12}^1 x_2 + w_{13}^1 x_3 + b_1^2) + w_{12}^2 (w_{21}^1 x_1 + w_{22}^1 x_2 + w_{23}^1 x_3 + b_2^2) + b_1^3 \\
&= x_1 (w_{11}^2 w_{11}^1 + w_{12}^2 w_{21}^1) + \\
&\quad x_2 (w_{11}^2 w_{12}^1 + w_{12}^2 w_{22}^1) + \\
&\quad x_3 (w_{11}^2 w_{13}^1 + w_{12}^2 w_{23}^1) + \\
&\quad w_{11}^2 b_1^2 + w_{12}^2 b_2^2 + b_1^3
\end{aligned} \tag{5.2}$$

which is a linear function on the input variables x_1, x_2, and x_3. It is easy to show that this observation generalizes to any arbitrary FFNN, as long as the neuron activation functions are linear.

Output layer: Lastly, FFNNs have an output layer that produces scores for the classes to be learned. Similar to the multiclass logistic regression, these scores can be aggregated into a probability distribution if the output layer includes a softmax function. However, the softmax function is optional (hence the dashed lines in the figure). If softmax is skipped, the class scores will not form a probability distribution, and they may or may not be bounded to the $[0, 1]$ interval depending on the activation functions used in the final layer.

The architecture shown in Figure 5.2 can be reduced to most of the classifiers we introduced so far. For example:

Perceptron: The Perceptron has no intermediate layers; has a single neuron in the output layer with a "pass through" activation function: $f(x) = x$; and no softmax.

Binary logistic regression Binary LR is similar to the Perceptron, with the only difference that the activation function of its output neuron is the sigmoid: $f = \sigma$.

Algorithm 7: Stochastic gradient descent algorithm for the training of neural networks.

```
1 initialize parameters in $\Theta$
2 while not converged do
3     for each training example $\mathbf{x}_i$ in $\mathbf{X}$ do
4         for each $\theta$ in $\Theta$ do
5             $\theta = \theta - \alpha \frac{d}{d\theta} C_i(\Theta)$
6         end
7     end
8 end
```

Multiclass logistic regression Multiclass LR has multiple neurons in its output layer (one per class); their activation functions are the "pass through" function, $f(x) = x$; and it has a softmax.

5.2 Learning Algorithm for Neural Networks

At a very high level, one can view a neural network as a complex machinery with many knobs, one for each neuron in the architecture. In this analogy, the learning algorithm is the operating technician whose job is to turn all the knobs to minimize the machine's output, i.e., the value of its cost function for each training example. If a neuron increases the probability of an incorrect prediction, its knob will be turned down. If a neuron increases the probability of a correct prediction, its knob will be turned up.

We will implement this learning algorithm that applies to any neural network with a generalization of the learning algorithm for multiclass logistic regression (Algorithm 6). The first key difference is that the parameters we are learning are no longer a single weight vector and a single bias term per class as in the multiclass LR. Instead, the neural network parameters contain one weight vector and one bias term for *each* neuron in an intermediate or final layer (see Figure 5.2). Because the number of these neurons may potentially be large, let's use a single variable name, Θ, to indicate the totality of parameters to be learned, i.e., all the weights and biases. We will also use θ to point to an individual parameter (i.e., one single bias term or a single weight) in Θ. Under these notations we can generalize Algorithm 6 into Algorithm 7, which applies to any neural network we will encounter in this book.[1]

Note that the key functionality remains exactly the same between Algorithms 6 and 7: in each iteration, both algorithms update their parameters by subtracting the partial derivative of the cost from their current values. As discussed, this guarantees that the cost function incre-

[1] We will revise this algorithm slightly in Chapter 6.

mentally decreases towards some local minimum. This observation is sufficient to understand how to implement the training algorithm for a FFNN using a modern machine learning library that includes auto-differentiation such as PyTorch. Thus, the impatient reader who wants to get to programming examples as quickly as possible may skip the remainder of this chapter and jump to the next one for code examples. However, we encourage the reader to stick around for the next sections in this chapter, where we will look "under the hood" of Algorithm 7 to understand better how it operates.

5.3 The Equations of Back-propagation

The key equation in Algorithm 7 is in row 5, which requires the computation of the partial derivative of the cost function for one training example $C_i(\Theta)$ with respect to *all* parameters in the network, i.e., all edge weights and all bias terms. While this looks mathematically simple, it is not intuitive: how are we to calculate the partial derivatives for parameters associated with neurons that are not in the final layer, and, thus, do not contribute directly to the cost function computation? To achieve this, we will implement an algorithm that has two phases: a *forward* phase, and a *backward* phase. In the forward phase, the algorithm runs the neural network with its current parameters to make a prediction on the given training example i. Using this prediction, we then compute the value of the cost function for this training example, $C_i(\Theta)$. Then, in the backward phase we incrementally propagate this information backwards, i.e., from the final layer towards the first layer, to compute the updates to the parameters in each layer. Because of this, this algorithm is commonly called *back-propagation*, or, for people in a hurry, *backprop*.

Let us formalize this informal description. To do this, we need to introduce a couple of new notations. First, because in this section we will use only one training example i and refer to the same training parameters Θ throughout, we will simplify $C_i(\Theta)$ to C in all the equations below. Second, and more importantly, we define the *error of neuron* i[2] in layer l as the partial derivative of the cost function with respect to the neuron's output:

$$\delta_i^l = \frac{d}{dz_i^l} C \tag{5.3}$$

where z_i^l is the output of neuron i in layer l before the activation function f is applied. Intuitively, the error of a neuron measures what impact a small change in its output z has on the cost C. Or, if we view z as a knob as in the previous analogy, the error indicates what impact turning the knob has. The error of a neuron is a critical component in backpropagation: we want to adjust the parameters of each neuron *proportionally* with the impact the neuron has on the cost function's value for this training example: the higher the impact, the bigger the adjustment. Lastly, we use the index L to indicate the *final* layer of the network, e.g., the

[2] Note that we are overloading the index i here. In Algorithm 7 we used it to indicate a specific training example $\mathbf{x}_i$. Now we use it to indicate a specific neuron.

Algorithm 8: The back-propagation algorithm that computes parameter updates for a neural network.

```
1 compute the errors in the final layer $L$, $\delta_i^L$, using the cost function $C$ (Equation 5.4)
2 backward propagate the computation of errors in all upstream layers (Equation 5.5)
3 compute the partial derivates of $C$ for all parameters in a layer $l$, $\frac{d}{db_i^l}C$ and $\frac{d}{dw_{ij}^l}C$, using
   the errors in the same layer, $\delta_i^l$ (Equations 5.6 and 5.7)
```

layer right before the softmax in Figure 5.2. Thus, δ_i^L indicates the error of neuron i in the final layer.

Using these notations, we formalize the backpropagation algorithm with the three steps listed in Algorithm 8. Step 1 computes the error of neuron i in the final layer as the partial derivative of the cost with respect to the neuron's activation multiplied with the partial derivative of the activation function with respect to the neuron's output:

$$\delta_i^L = \frac{d}{da_i^L} C \frac{d}{dz_i^L} f(z_i^L) \tag{5.4}$$

This equation may appear daunting at first glance (two partial derivatives!), but it often reduces to an intuitive formula for given cost and activation functions. As a simple example, consider the case of binary classification, i.e., a single neuron in the final layer with a sigmoid activation (and no softmax), coupled with the mean squared error (MSE) cost function, a simple cost function commonly used for binary classification: $C = \frac{1}{2}(y - a_1^L)^2$, where y is the gold label for the current training example, i.e., 0 or 1 for binary classification. That is, the MSE cost simply minimizes the difference between the prediction of the network and the gold label. The derivative of the MSE cost with respect to the neuron's activation is: $\frac{d}{da_1^L}C = a_1^L - y$.[3] The derivative of the sigmoid with respect to the neuron's output is: $\frac{d}{dz_1^L}\sigma(z_1^L) = \sigma(z_1^L)(1-\sigma(z_1^L))$ (see Table 3.1). Thus, δ_1^L in this simple example is computed as: $\delta_1^L = (a_1^L - y)\sigma(z_1^L)(1-\sigma(z_1^L)) = (\sigma(z_1^L) - y)\sigma(z_1^L)(1-\sigma(z_1^L))$. It is easy to see that this error formula follows our knob analogy: when the activation of the final neuron is close to the gold label y, which can take values of 0 or 1, the error approaches 0 because two of the terms in its product are close to 0. In contrast, the error value is largest when the classifier is "confused" between the two classes, i.e., its activation is 0.5. The same can be observed for any (differentiable) cost and activation functions (see next chapter for more examples).

[3] This is trivially derived by applying the chain rule.

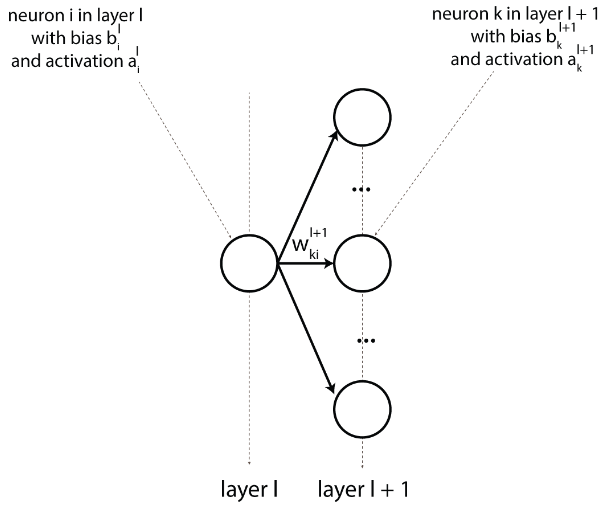

Figure 5.4 Visual helper for Equation 5.5.

Equation 5.4 is easy to prove using a direct application of the chain rule:

$$\begin{aligned}\delta_i^L &= \sum_k \frac{d}{da_k^L} C \frac{d}{dz_i^L} a_k^L \\ &= \frac{d}{da_i^L} C \frac{d}{dz_i^L} a_i^L\end{aligned}$$

where *k* iterates over all neurons in the last layer. Note that we need to sum over all neurons in the final layer in the first line of the proof because *C* theoretically depends on all activations in the final layer. However, neuron *i* impacts only its own activation, and, thus, we can ignore all other activations (second line of the proof).

Equation 5.4 computes the errors in the *last* layer of the network. The next back-propagation equation incrementally propagates the computation of errors into the upstream layers, i.e., the layers that are farther to the left in Figure 5.2. That is, this equation computes the errors in a layer l using the errors in the layer immediately downstream, $l+1$, as follows:

$$\delta_i^l = \sum_k \delta_k^{l+1} w_{ki}^{l+1} \frac{d}{dz_i^l} f(z_i^l) \tag{5.5}$$

where k iterates over all neurons in layer $l+1$.

We prove this equation by first applying the chain rule to introduce the outputs of the downstream layer, z_k^{l+1}, in the formula for the error of neuron i in layer l, and then taking advantage of the fact the outputs in the downstream layer $l+1$ depend on the activations in the previous layer l. More formally:

$$
\begin{aligned}
\delta_i^l &= \frac{d}{dz_i^l} C \\
&= \sum_k \frac{d}{dz_k^{l+1}} C \frac{d}{dz_i^l} z_k^{l+1} \\
&= \sum_k \delta_k^{l+1} \frac{d}{dz_i^l} z_k^{l+1} \\
&= \sum_k \delta_k^{l+1} \frac{d}{dz_i^l} (\sum_j w_{kj}^{l+1} a_j^l + b_k^{l+1}) \\
&= \sum_k \delta_k^{l+1} \frac{d}{dz_i^l} (w_{ki}^{l+1} a_i^l) \\
&= \sum_k \delta_k^{l+1} w_{ki}^{l+1} \frac{d}{dz_i^l} a_i^l \\
&= \sum_k \delta_k^{l+1} w_{ki}^{l+1} \frac{d}{dz_i^l} f(z_i^l)
\end{aligned}
$$

where j iterates over all neurons in layer l. Similar to the previous proof, we need to sum over all the neurons in layer $l+1$ (second line of the proof) because the value of the cost function is impacted by all the neurons in this layer. The rest of the proof follows from the fact that $z_k^{l+1} = \sum_j w_{kj}^{l+1} a_j^l + b_k^{l+1}$. Figure 5.4 provides a quick visual helper to navigate the indices used in this proof.

Using Equations 5.4 and 5.5 we can compute the errors of all neurons in the network. Next we will use these errors to compute the partial derivatives for all weights and bias terms in the network, which we need for the stochastic gradient descent updates in Algorithm 7. First, we compute the partial derivative of the cost with respect to a bias term as:

$$\frac{d}{db_i^l} C = \delta_i^l \tag{5.6}$$

The proof of this equation follows similar steps with the previous two proofs, but here we iterate over neurons in the same layer l (so we can access the error of neuron i). Thus, we can ignore all neurons other than neuron i, which depends on this bias term:

$$\begin{aligned}\frac{d}{db_i^l}C &= \sum_k \frac{d}{dz_k^l}C\frac{d}{db_i^l}z_k^l \\ &= \frac{d}{dz_i^l}C\frac{d}{db_i^l}z_i^l \\ &= \delta_i^l\frac{d}{db_i^l}z_i^l \\ &= \delta_i^l\frac{d}{db_i^l}(\sum_h w_{ih}^l a_h^{l-1} + b_i^l) \\ &= \delta_i^l\end{aligned}$$

where k iterates over all neurons in layer l, and h iterates over the neurons in layer $l-1$.

Similarly, we compute the partial derivative of the cost with respect to the weight that connects neuron j in layer $l-1$ with neuron i in layer l, $\frac{d}{dw_{ij}^l}C$, as:

$$\frac{d}{dw_{ij}^l}C = a_j^{l-1}\delta_i^l \tag{5.7}$$

The proof of this equation follows the same structure as the proof above:

$$\begin{aligned}\frac{d}{dw_{ij}^l}C &= \sum_k \frac{d}{dz_k^l}C\frac{d}{dw_{ij}^l}z_k^l \\ &= \frac{d}{dz_i^l}C\frac{d}{dw_{ij}^l}z_i^l \\ &= \delta_i^l\frac{d}{dw_{ij}^l}z_i^l \\ &= \delta_i^l\frac{d}{dw_{ij}^l}(\sum_h w_{ih}^l a_h^{l-1} + b_i^l) \\ &= \delta_i^l a_j^{l-1}\end{aligned}$$

where k iterates over all neurons in layer l, and h iterates over the neurons in layer $l-1$.

Equations 5.4 to 5.7 provide a formal framework to update the parameters of any neural network (weights and biases). They also highlight several important observations:

1. Implementing a basic feed forward neural network is not that complicated. Equations 5.4 to 5.7 rely on only two derivatives: the derivative of the activation function f, and the derivative of the cost function. In theory, these could be hard-coded for the typical activation and cost functions to be supported. The rest of the mathematical operations needed to implement back-propagation are just additions and multiplications. However, in practice, there are some additional issues that need to be addressed for a successful neural network implementation. We will discuss these issues in Chapter 6.

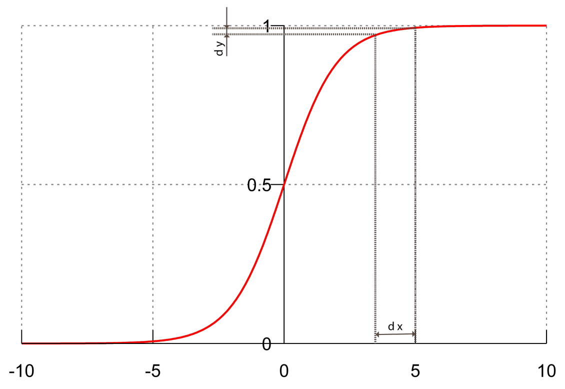

Figure 5.5 Visualization of the vanishing gradient problem for the sigmoid function: changes in x yield smaller and smaller changes in y at the two ends of the function, which means that $\frac{d}{dx}\sigma$ approaches zero in the two extremes.

2. Back-propagation is slow. As shown in the equations, updating the network parameters requires a considerable number of multiplications. For real-world neural networks that contain millions of parameters this becomes a significant part of the training runtime. In the next chapters we will discuss multiple strategies for speeding up the training process such as batching multiple training examples and multiple operations together (e.g., updating all bias terms in a layer with a single vector operation rather than several scalar updates as in the equations). When these tensor operations are moved onto a graphics processing unit (GPU), which has hardware support for parallel tensor operations, they can be executed much faster.
3. Depending on the activation function, its partial derivative with respect to model parameters may be too small, which slows down the learning process considerably. This happens because the equations to compute the errors in the network layers (Equations 5.4 and 5.5) both depend on this derivative. Multiplying this derivative repeatedly, as required by the recursive process described in the two equations, may have the unintended side effect that some errors will approach zero, which, in turn, means that the network parameters will not be updated in a meaningful way. This phenomenon is commonly called the "vanishing gradient problem." Figure 5.5 shows a visualization of this phenomenon for the sigmoid activation function. For this reason, other activations that are more robust to this problem are commonly used in deep learning. We will discuss some these in Chapter 6.

5.4 Drawbacks of Neural Networks (So Far)

In this chapter we generalized logistic regression into multi-layered neural networks, which can learn nonlinear functions. This is a major advantage over LR, but it can be also be a drawback: because of their flexibility, neural networks can "hallucinate" classifiers that fit the training data well, but fail to generalize to previously unseen data [**?**]. This process is called *overfitting*. We will discuss multiple strategies to mitigate overfitting in Chapter 6.

In addition of overfitting, the training process of neural networks may suffer from other problems. We discussed the vanishing gradient problem in the previous section. Another problem commonly observed when training neural networks is the tendency to "Tony Hawk" the data, which slows down convergence, or prevents it all together. Chapter 6 discusses optimization algorithms that reduce this phenomenon.

Further, similar to the Perceptron and LR, the neural networks covered so far continue to rely on hand-crafted features. We will address this limitation in Chapter 8. Lastly, feed forward neural networks focus on individual predictions rather than structured learning (i.e., where multiple predictions such as the part-of-speech in a sentence are jointly generated). We will start introducing structured prediction using neural networks in Chapter 12. This will open the door to other important NLP applications such as part-of-speech tagging, named entity recognition, or syntactic parsing.

5.5 Historical Background

TODO: To do

5.6 References and Further Readings

TODO: To do

6 Best Practices in Deep Learning

7 Implementing the Review Classifier with Feed Forward Networks in PyTorch

8 Distributional Hypothesis and Representation Learning

As mentioned in the previous chapters, all the algorithms we covered so far rely on hand-crafted features that must be designed and implemented by the machine learning developer. This is problematic for two reasons. First, designing such features can be a complicated endeavor. For example, even for the apparently simple task of designing features for text classification questions arise quickly: How should we handle syntax? How do we model negation? Second, most words in any language tend to be very infrequent. This was formalized by **?**, who observed that if one ranks the words in a language in descending order of their frequency then the frequency of the word at rank i is $\frac{1}{i}$ times the frequency of the most frequent word. For example, the most frequent word in English is *the*. The frequency of the second most frequent word according to Zip's law is half the frequency of *the*; the frequency of the third most-frequent word is one third of the frequency of *the*, and so on.[1] In our context, this means that most words are very sparse, and our text classification algorithm trained on word-occurrence features may generalize poorly. For example, if the training data for a review classification dataset contains the word *great* but not the word *fantastic*, a learning algorithm trained on this data will not be able to properly handle reviews containing the latter word, even though there is a clear semantic similarity between the two. In the wider field of machine learning, this problem is called the "curse of dimensionality" [**?**].

In this chapter we will begin to addresses this limitation. In particular, we will discuss methods that learn numerical representations of words that capture some semantic knowledge. Under these representations, similar words such as *great* and *fantastic* will have similar forms, which will improve the generalization capability of our ML algorithms.

8.1 Traditional Distributional Representations

The methods in this section are driven by the distributional hypothesis of **?**, who observed that words that occur in similar contexts tend to have similar meanings. The same idea was popularized a few years later by **?** who, perhaps more elegantly, stated that "a word is characterized by the company it keeps." It is easy to intuitively demonstrate the distributional

[1] Interestingly, this law was observed to hold even for non-human languages such as dolphin whistles [**?**].

hypothesis. For example, when presented with the phrases *bread and …* and *bagels with …*, many people will immediately guess from the provided context that the missing words are *butter* and *cream cheese*, respectively.

In this section, we will formalize this observation. In particular, we will associate each word in a given vocabulary with a vector, which represents the context in which the word occurs. According to the distributional hypothesis these vectors should capture the semantic meaning of words, and, thus, words that are similar should have similar vectors.

Traditionally, these vectors were built simply as co-occurrence vectors. That is, for each word w in the vocabulary, its vector counts the co-occurrence with other words in its surrounding context, where this context is defined as a window of size $[-c, +c]$ words around all instances of w in text. Here, we use negative values to indicate number of words to the left of w, and positive values to indicate number of words to the right. For example, consider the text below:

> *A bagel and cream cheese (also known as bagel with cream cheese) is a common food pairing in American cuisine. The bagel is typically sliced into two pieces, and can be served as-is or toasted.*[2]

In this text, *bagel* occurs three times. Thus, we will have three context windows, one for each mention of the word. While common values for c range from 10 to 20, let us set $c = 3$ for this simple example. Under this configuration, the three context windows for *bagel* in this text are:

- *A* bagel *and cream cheese*
- *also known as* bagel *with cream cheese*
- *American cuisine The* bagel *is typically sliced*

Note that we skipped over punctuation signs when creating these windows.[3] If we aggregate the counts of words that appear in these context windows, we obtain the following co-occurrence vector for *bagel*:

A	also	American	and	as	cheese	cream	cuisine	is	known	sliced	The	typically	with
1	1	1	1	1	2	2	1	1	1	1	1	1	1

This example shows that the co-occurrence vector indeed captures meaningful contextual information: *bagel* is most strongly associated with *cream* and *cheese*, but also with other relevant context words such as *cuisine* and *sliced*. The larger the text used to compute these co-occurrence vectors is, the more meaningful these vectors become.

[2] Text adapted from the *Bagel and cream cheese* Wikipedia page: https://en.wikipedia.org/wiki/Bagel_and_cream_cheese.

[3] Different ways of creating these context windows are possible. For example, one may skip over words deemed to contain minimal semantic meaning such as determiners, pronouns, and prepositions. Further, these windows may be restricted to content within the same sentence. Lastly, words may be normalized in some form, e.g., through lemmatization. We did not use any of these heuristics in our example for simplicity.

In practice, these co-occurrence vectors are generated from large document collections such as a dump of Wikipedia,[4] and are constructed to have size M, where M is the size of entire word vocabulary, i.e., the totality of the words observed in the underlying document collection. Note that these vectors will be sparse, i.e., they will contain many zero values, for all the words in the vocabulary that do not appear in the context of the given word. Having all co-occurrence vectors be of similar size allows us to formalize the output of this whole process into a single co-occurrence matrix $\mathbf{C}$ of dimension $M \times M$, where row i corresponds to the co-occurrence vector for word i in the vocabulary. A further important advantage of standardizing vector sizes is that we can easily perform vector operations (e.g., addition, dot product) between different co-occurrence vectors, which will become important soon.

Once we have this co-occurrence matrix, we can use it to improve our text classification algorithm. That is, instead of relying on an explicit feature matrix (see, for example, the feature matrix in Table 2.4), we can build our classifier on top of the co-occurrence vectors. A robust and effective strategy to this end is to simply average the co-occurrence vectors for the words contained in a given training example [**?**]. Take, for example, the first training example in Table 2.4: instead of training on the sparse feature vector listed in the first row in the table, we would train on a new vector that is the average of the context vectors for the three words present in the training example: *good*, *excellent*, and *bad*. This vector should be considerably less sparse than the original feature vector, which contains only three non-zero entries. The fist obvious consequence of this decision is that the dimensions of the classifier's parameters change. For example, in the case of a Perceptron or a logistic regression, the dimension of the vector $\mathbf{w}$ becomes M to match the dimension of the co-occurrence vectors. The second, more important consequence, is that the parameter vector $\mathbf{w}$ becomes less sparse because it is updated with training examples that are less sparse in turn. This means that our new classifier should generalize better to other, previously unseen words. For example, we expect other words that carry positive sentiment to occur in similar contexts with *good* and *excellent*, which means that the dot product of their co-occurrence vectors with the parameter $\mathbf{w}$ is less likely to be zero.

8.2 Matrix Decompositions and Low-rank Approximations

But have we really solved the "curse of dimensionality" by using these co-occurrence vectors instead of the original lexical features? One may reasonably argue that we have essentially "passed the buck" from the explicit lexical features, which are indeed sparse, to the co-occurrence vectors, which are probably less sparse, but most likely have not eliminated the sparsity curse. This is intuitively true: consider the co-occurrence vector for the word *bagel* from our previous example. Regardless of how large the underlying document collection used to compute these vectors is and how incredible bagels are, it is very likely that the context

[4] https://www.wikipedia.org

vector for *bagel* will capture information about breakfast foods, possibly foods in general and other meal-related activities, but will not contain information about the myriad other topics that occur in these documents in bagel-free contexts.

To further mitigate the curse of dimensionality, we will have to rely on a little bit of linear algebra. Without going into mathematical details, it is possible to decompose the co-occurrence matrix **C** into a product of three matrices:

$$\mathbf{C} = \mathbf{U}\Sigma\mathbf{V}^T \tag{8.1}$$

where **U** has dimension $M \times r$, Σ is a squared matrix of dimension $r \times r$, and $\mathbf{V}^T$ has dimension $r \times M$.[5] Each of these three matrices has important properties. First, Σ is a diagonal matrix. That is, all its elements are zero with the exception of the elements on the diagonal: $\sigma_{ij} = 0$ for $i \neq j$.[6] The non-zero diagonal values, σ_{ii}, are referred to as the *singular values* of **C**, and, for this reason, this decomposition of **C** is called *singular value decomposition* or SVD.[7] The dimension of Σ, r, is called the *rank* of the matrix **C**.[8] Importantly, as we will see in a minute, the values σ_{ii} are listed in descending order in Σ. That is, $\sigma_{ii} > \sigma_{jj}$ for $i < j$. Further, the rows in **U** are orthogonal, i.e., the dot product of any two rows in **U** is zero. Similarly, the rows in **V** (or columns in $\mathbf{V}^T$) are also orthogonal.

So, where does all this math leave us? It turns out that the output of the singular value decomposition process has important linguistic interpretations (see Figure 8.1 for a summary):

1. Each row in the matrix **U** contains the numerical representation of a single word in the vocabulary, and each column in **U** is one semantic dimension, or topic, used to describe the underlying documents that were used to construct **C**. For example, if row i contains the co-occurrence vector for the word *bagel* and column j contains a topic describing foods, we would expect c_{ij} to have a high value because the food topic is an important part of the semantic description of the word *bagel*. Importantly however, the SVD algorithm does not guarantee that the semantic dimensions encoded as columns in **U** are actually interpretable to human eyes. Assigning meaning to these dimensions is a post-hoc, manual process that requires the inspection of the $\mathbf{V}^T$ matrix (see third item).

[5] The superscript T indicates the transpose operation. It is used here to indicate that $\mathbf{V}^T$ is computed as the transpose of another matrix **V**, which has certain mathematical properties. This is less important for our discussion. But we keep the same notation as the original algorithm, for consistency.

[6] For those of us not familiar with the Greek alphabet, σ and Σ are lowercase/uppercase forms of the Greek letter sigma. We use the former to indicate elements in the latter matrix.

[7] The general form of singular value decomposition does not require the matrix **C** to be square. For this reason, the SVD form we discuss here, which relies on a square matrix **C**, is referred to as *truncated* singular value decomposition. In this book, we will omit the *truncated* modifier, for simplicity.

[8] In general, the rank of a matrix **C** is equal to the number of rows in **C** that are linearly independent of each other, i.e., they cannot be computed as a linear combination of other rows. This is not critical to our discussion.

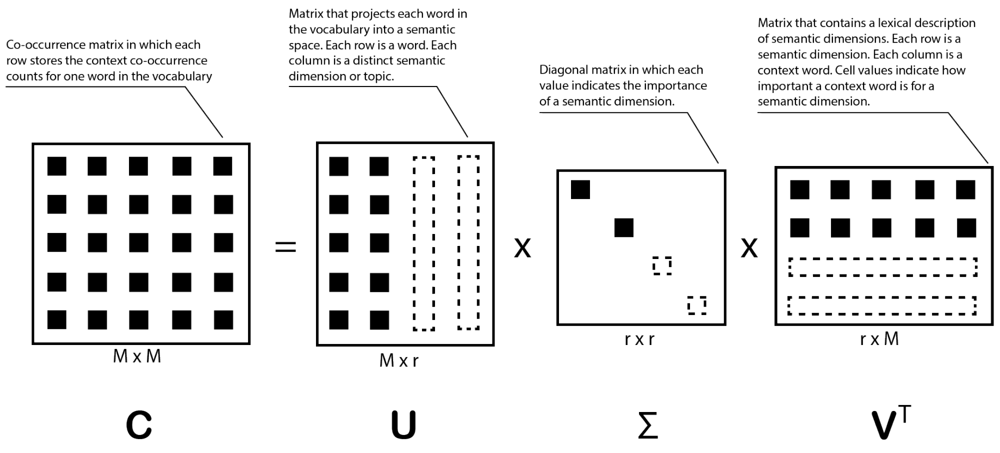
Co-occurrence matrix in which each row stores the context co-occurrence counts for one word in the vocabulary
Matrix that projects each word in the vocabulary into a semantic space. Each row is a word. Each column is a distinct semantic dimension or topic.
Diagonal matrix in which each value indicates the importance of a semantic dimension.
Matrix that contains a lexical description of semantic dimensions. Each row is a semantic dimension. Each column is a context word. Cell values indicate how important a context word is for a semantic dimension.
M x M
M x r
r x r
r x M
=
X
X
C
U
Σ
V^T

Figure 8.1 Summary of the four matrices in the singular value decomposition equation: $\mathbf{C} = \mathbf{U}\Sigma\mathbf{V}^T$. The empty rectangles with dashed lines indicate which elements are zeroed out under the low-rank approximation.

2. The singular values in Σ indicate the importance of topics captured in $\mathbf{U}$. That is, if $\sigma_{ii} > \sigma_{jj}$ then topic i (i.e., the column i in $\mathbf{U}$) is more important than column j. And, since the values in Σ are listed in descending order, we can state that topic i is more important than topic j, if $i < j$. This will become important in a minute.
3. Each row i in $\mathbf{V}^T$ contains a bag-of-words description of topic i, where the value at position j in row i indicates the importance of word j to topic i. For example, if the three highest values in a given row point to the words *bagel*, *bread*, and *croissant*, one can (subjectively) interpret this topic to be about bakery products. As mentioned before, such interpretations are not always easy to make. Because the SVD algorithm is completely agnostic to linguistic interpretations, it is possible that some of the produced topics will resist an immediate interpretation. This is an unfortunate drawback we will have to live with, for the sake of mitigating the curse of dimensionality.

While the SVD process produces a new vector representation for each word in the vocabulary, i.e., row i in the matrix $\mathbf{U}$ corresponds to the new representation of word i, we are not quite done. The rank of the matrix $\mathbf{C}$, r, which also indicates the number of columns in $\mathbf{U}$, is guaranteed to be smaller than M, but it is not necessarily much smaller. We would like to produce vector representations of dimension k, where k is much smaller than M, $k \ll M$. To generate these representations, we will take advantage of the fact that, as discussed, the diagonal matrix Σ contains the topic importance values listed from largest to smallest. Thus, intuitively, if one were to remove the *last* $r-k$ topics we would not lose that much information because the top k topics that are most important to describe the content of $\mathbf{C}$ are still present. Formally, this can be done by zeroing out the last $r-k$ elements of Σ, which has the effect of ignoring the last $r-k$ columns in $\mathbf{U}$ and the last $r-k$ rows in $\mathbf{V}^T$ in the SVD multiplication. Figure 8.1 visualizes this process using empty squares and rectangles for the elements in Σ and rows/columns in $\mathbf{U}/\mathbf{V}^T$ that are zeroed out. The resulting matrix $\mathbf{C}$ that is generated when only the first k topics are used is called a *low-rank approximation* of the original matrix $\mathbf{C}$. To distinguish between the two matrices, we will use the notation $\mathbf{C}_k$ to denote the low-rank approximation matrix. There is theory that demonstrates that $\mathbf{C}_k$ is the best approximation of $\mathbf{C}$ for rank k. What this means for us is that we can use the first k columns in $\mathbf{U}$ to generate numerical representations for the words in the vocabulary that approximate as well as possible the co-occurrence counts encoded in $\mathbf{C}$. In empirical experiments, k is typically set to values in the low hundreds, e.g., 200. This means that, once this process is complete, we have associated each word in the vocabulary with a vector of dimension $k = 200$ that is its numerical representation according to the distributional hypothesis.

8.3 Drawbacks of Representation Learning Using Low-Rank Approximation

Although this approach has been demonstrated empirically to be useful for several NLP applications including text classification and search, it has two major problems. The first is that this method, in particular the SVD component, is expensive. Without going into mathematical details, we will mention that the cost of the SVD algorithm is cubic in the dimension of $\mathbf{C}$. Since in our case the dimension of $\mathbf{C}$ is the size of the vocabulary, M, our runtime cost is proportional to M^3. In many NLP tasks the vocabulary size is in the hundreds of thousands of words (or more!), so this is clearly a very expensive process. The second drawback is that this approach conflates all word senses into a single numerical representation. For example, the word *bank* may mean a financial institution, or sloping land, e.g., as in *bank of the river*. But because the algorithm that generates the co-occurrence counts is not aware of the various senses of a given word, all these different semantics are conflated into a single vector. We will address the first drawback in the remaining part of this chapter, and the second in Chapter 10.

8.4 The Word2vec Algorithm

The runtime cost of learning word numerical representations has been addressed by **?**, who proposed the word2vec algorithm.[9] Similar to our previous discussion, the goal of this algorithm is to learn numerical representations that capture that distributional hypothesis. More formally, word2vec introduces a training objective that learns "word vector representations that are good at predicting the nearby words." In other words, this algorithm flips the distributional hypothesis on its head. While the original hypothesis stated that "a word is characterized

[9] The name of this algorithm is an abbreviation of "word to vector."

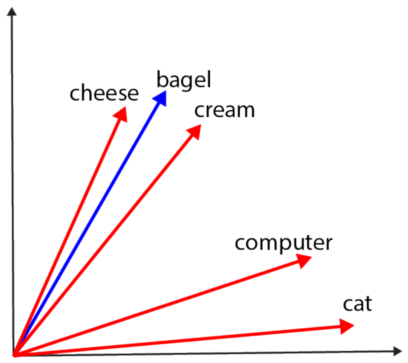

Figure 8.2 An illustration of the word2vec algorithm, the skip-gram variant, for the word *bagel* in the text: *A bagel and cream cheese (also known as bagel with cream cheese) is a common food pairing in American cuisine.* Blue indicates “input” vectors; red denotes “output” vectors. The algorithm clusters together output vectors for the words in the given context window (e.g., *cream* and *cheese*) with the corresponding input vector (*bagel*), and pushes away output vectors for words that do not appear in its proximity (e.g., *computer* and *cat*).

by the company it keeps,” i.e, a word is defined by its context, word2vec’s training objective predicts the context in which a given word is likely to occur, i.e., the context is defined by the word. **?** proposed two variants of word2vec. For simplicity, we will describe here the variant called “skip-gram,” which implements the above training objective. From here on, we will refer to the skip-gram variant of word2vec simply as word2vec.

Figure 8.2 illustrates the intuition behind word2vec’s training process. Visually, the algorithm matches the distribution hypothesis exactly: it makes sure that the vector representation of a given word (e.g., *bagel* in the example shown in the figure) is close to those of words that appear near the given word (e.g., *cream* and *cheese*), and far from the vector representations of words that do not appear in its neighborhood (e.g., *computer* and *cat*). Importantly, to distinguish between input words and context words, the algorithm actually learns two vectors for each word in the vocabulary: one for when it serves as an input word (e.g., *bagel* in the example), and one for when it serves as a context our output word (e.g., *cheese*).

More formally, the algorithm implements the distributional hypothesis as a prediction task. First, for each input word w_i in the vocabulary,[10] the algorithm identifies the context windows of size $[-c, +c]$ around all instances of w_i in some large text. This process is identical to the way we constructed the context windows at the beginning of this chapter. For example, the first context window for the word *bagel* and $c = 3$ is: *A* bagel *and cream cheese*. Second, all the context (or output) words that appear in these windows are added to the pool of words that

[10] In practice, the algorithm uses only the most frequent k words in the vocabulary to reduce training run times.

should be predicted given w_i. Then, the training process maximizes the prediction probability for each word w_j in the context of w_i. That is, the theoretical[11] cost function C for word2vec is:

$$C = -\sum_{i=1}^{M} \sum_{w_j \text{ in the context of } w_i} \log(p(w_j|w_i)) \tag{8.2}$$

where the probability $p(w_j|w_i)$ is computed using the input vector for w_i, the output vector for w_j and the softmax function introduced in Section 3.5:

$$p(w_j|w_i) = \frac{e^{\mathbf{v}^o_{w_j} \cdot \mathbf{v}^i_{w_i}}}{\sum_{k=1}^{M} e^{\mathbf{v}^o_{w_k} \cdot \mathbf{v}^i_{w_i}}} \tag{8.3}$$

where $\mathbf{v}^i$ indicates an input vector (i.e., the blue vectors in Figure 8.2), $\mathbf{v}^o$ indicates a context vector (red vectors in the figure), and the denominator in the fraction iterates over all the words in the vocabulary of size M in order to normalize the resulting probability. All $\mathbf{v}^i$ and $\mathbf{v}^o$ vectors are updated using the standard stochastic gradient descent algorithm during training, similar to the procedure described in Chapter 3. That is, each weight u from a $\mathbf{v}^i$ and $\mathbf{v}^o$ vector is updated based on its partial derivative, $\frac{d}{du}C_i$, where C_i is the loss function for input word i in the vocabulary: $C_i = -\sum_{w_j \text{ in the context of } w_i} \log(p(w_j|w_i))$.

It is important to note at this stage that the last two equations provide a formalization of the intuition shown in Figure 8.2. That is, minimizing the cost function C has the effect of maximizing the probabilities $p(w_j|w_i)$ due to the negative sign in Equation 8.2. Further, maximizing these probabilities has the consequence of bringing the output vectors of context words ($\mathbf{v}^o_{w_j}$) and the input vector for word w_i ($\mathbf{v}^i_{w_i}$) closer together because that maximizes the dot product in the numerator in Equation 8.3. Similarly, maximizing these probabilities has the effect of minimizing the denominator of the fraction in Equation 8.3, which, in turn, means that the dot products with vectors of words *not* in the context of w_i will be minimized.

A second important observation is that there is a very close parallel between this algorithm and the multi-class logistic regression algorithm introduced in Section 3.5. Similar to the multi-class LR algorithm, here we use data points described through a vector representation ($\mathbf{v}^i$ here vs. $\mathbf{x}$ in the standard LR algorithm) to predict output labels (context words vs. labels in $\mathbf{y}$ for LR). Both algorithms have the same cost function: the negative log likelihood of the training data. However, there are three critical differences between word2vec and multi-class LR:

Difference #1: while the formulas for the dot products in the two algorithms look similar, in LR the $\mathbf{x}$ is static, i.e., it doesn't change during training, whereas in word2vec both $\mathbf{v}^i$ and $\mathbf{v}^o$

[11] We call this cost function "theoretical" because, as we will see in a minute, this is not what is actually implemented.

vectors are dynamically adjusted through stochastic gradient descent. This is because the **x** vector in LR stores explicit features that describe the given training example (and thus does not change), whereas in word2vec both $\mathbf{v}^i$ and $\mathbf{v}^o$ vectors are continuously moved around in their multi-dimensional space during training to match the distributional hypothesis in the training dataset. For this reason, the word2vec algorithm is also referred to as "dynamic logistic regression."

Difference #2: the **x** vector in LR stores explicit features whereas the weights u in the $\mathbf{v}^i$ and $\mathbf{v}^o$ vectors in word2vec are simply coordinates in a multi-dimensional space. For this reason, the output of the word2vec training process is considerably less interpretable than that of LR. For example, in multi-class LR, one can inspect the largest weights in the learned vector $\mathbf{w}_c$ for class c to identify the most important features for the classification of class c. This is not possible for word2vec. Further, word2vec is even less interpretable than the singular value decomposition matrix **U** in Section 8.2. There we could use the $\mathbf{V}^T$ matrix to come up with a (subjective) interpretation of each column in **U**. Again, this is not possible in word2vec, where no such descriptions exist.

Difference #3: Lastly, the number of classes in a multi-class LR problem is usually much smaller than the number of context words in word2vec, which is equal to the size of the vocabulary, M. Typically the former is tens or hundreds, whereas M may be in the millions or billions. Because of this, the denominator of the conditional probability in Equation 8.3 is prohibitively expensive to calculate. Due to this, the actual word2vec algorithm does not implement the cost function in Equation 8.2 but an approximated form of it:

$$C = -\sum_{i=1}^{M}\Big(\sum_{w_j \text{ in the context of } w_i} \log(\sigma(\mathbf{v}^o_{w_j}\cdot\mathbf{v}^i_{w_i})) + \sum_{w_j \text{ not in the context of } w_i} \log(\sigma(-\mathbf{v}^o_{w_j}\cdot\mathbf{v}^i_{w_i}))\Big) \tag{8.4}$$

or, for a single input word w_i:

$$C_i = -\Big(\sum_{w_j \in P_i} \log(\sigma(\mathbf{v}^o_{w_j}\cdot\mathbf{v}^i_{w_i})) + \sum_{w_j \in N_i} \log(\sigma(-\mathbf{v}^o_{w_j}\cdot\mathbf{v}^i_{w_i}))\Big) \tag{8.5}$$

where σ is the standard sigmoid function, $\sigma(x) = \frac{1}{1+e^{-x}}$, P_i is the set of context words for the input word w_i, and N_i is the set of words *not* in the context of w_i.

This new cost function captures the same distributional hypothesis: the first sigmoid maximizes the proximity of input vectors with the output vectors of words in context, whereas the second sigmoid minimizes the proximity of input vectors to output vectors of words not in context, due to the negative sign in the sigmoid parameter: $-\mathbf{v}^o_{w_j}\cdot\mathbf{v}^i_{w_i}$. However, this cost function is much easier to compute than the first cost function in Equation 8.2 for two reasons. First, we are no longer using conditional probabilities, which are expensive to normalize. Second, the right-most term of the cost function in Equation 8.5 does not operate

Algorithm 9: word2vec training algorithm.

```
for each word $w_i$ in the vocabulary do
    initialize $\mathbf{v}^i_{w_i}$ and $\mathbf{v}^o_{w_i}$ randomly
end
while not converged do
    for each word position i in the training dataset do
        $w_i$ = word at position $i$
        $P_i$ = set of words in the window $[i-c, i+c]$ around $w_i$
        $N_i$ = sampled from the set of words not in $P_i$
        compute cost function $C_i$ using $P_i$, $N_i$ and Equation 8.5
        for each dimension u in $\mathbf{v}^i_{w_i}$ do
            $u = u - \alpha \frac{d}{du} C_i$
        end
        for each word $w_j \in P_i \cup N_i$ do
            for each dimension u in $\mathbf{v}^o_{w_j}$ do
                $u = u - \alpha \frac{d}{du} C_i$
            end
        end
    end
end
for each word $w_i$ in the vocabulary do
    return $(\mathbf{v}^i_{w_i} + \mathbf{v}^o_{w_i})/2$
end
```

over all the words in the vocabulary, but over a small sample of words that do not appear in the context of w_i. These words can be selected using various heuristics. For example, one can uniformly choose words from the training dataset such that they do not appear in the context of a given input word w_i. However, this has the drawback that it will oversample very frequent words (which are more common and, thus, more likely to be selected). To control for this, the word2vec algorithm selects a non-context word w proportional to the probability $p(w) = \frac{freq(w)^{3/4}}{Z}$, where $freq(w)$ indicates the frequency of word w in the training corpus, and Z is the total number of words in this corpus. The only difference between the probability $p(w)$ and the uniform probability is the $3/4$ exponent. This exponent dampens the importance of the frequency term, which has the effect that very frequent words are less likely to be oversampled.

Algorithm 9 lists the pseudocode for the complete training procedure for word2vec that incorporates the discussion above. This algorithm is another direct application of stochastic gradient descent, which is used to update both the input vectors (lines 10 – 12) and output vectors (lines 13 – 17) until convergence (or for a fixed number of epochs). In all update equations, α indicates the learning rate. At the end, the algorithm returns the average of the input and output vectors as the numeric representation of each word in the vocabulary (lines 20 – 22). Note that other ways of computing the final word numeric representations are possible, but the simple average has been observed to perform well in practice for downstream tasks [**?**].

In addition to the more efficient cost function, this algorithm has a second practical simplification over our initial discussion. The algorithm does not identify all context windows for each word in the vocabulary ahead of time, as we discussed when we introduced the cost function in Equation 8.2. This would require complex bookkeeping and, potentially, a considerable amount of memory. Instead, Algorithm 9 linearly scans the text (line 5), and constructs a *local* context P_i and a negative context N_i from the current context window at this position in the text (lines 7 and 8). This has several advantages. First, since only one pair of local P_i and N_i sets are kept in memory at a time, the memory requirements for this algorithm are much smaller. Second, the runtime cost of this algorithm is linear in the size of the training dataset because (a) all operations in the inner `for` loop depend on the size of the context window, which is constant (lines 6 – 17), and (b) the number of epochs used in the external `while` loop (line 4) is a small constant. This is a tremendous improvement over the runtime of the SVD procedure, which is cubic in the size of the vocabulary. One potential drawback of this strategy is that the local N_i used in the algorithm may not be accurate. That is, the words sampled to be added to N_i in line 8 may actually appear in another context window for the another instance of the current word in the training dataset. However, in practice, this does not seem to be a major problem.

The vectors learned by word2vec have been shown to capture semantic information that has a similar impact on downstream applications as the vectors learned through the more expensive low-rank approximation strategy discussed earlier in this chapter [**?**]. We will discuss some of these applications in the following chapters. This semantic information can also be directly analyzed. For example, **?** showed that a visualization of 1000-dimensional vectors learned by word2vec surfaces interesting patterns. For example, the relation between countries and their capital cities (shown as the difference between the two respective vectors) tends to be same regardless of country and capital (Figure 8.3). That is, $\vec{China} - \vec{Beijing} \approx \vec{Portugal} - \vec{Lisbon}$, where the superscript arrow indicates the vector learned by word2vec for the corresponding word. Many other similar patterns have been observed. For example, the difference between the vectors of *king* and *man* is similar to the difference between the vectors of *queen* and *woman*: $\vec{king} - \vec{man} \approx \vec{queen} - \vec{woman}$, which suggests that this difference captures the semantic representation of a genderless monarch. In the following chapters, we

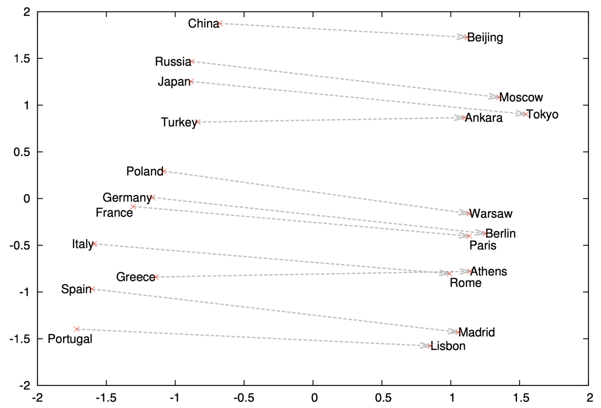

Figure 8.3 Two-dimensional projection of 1000-dimensional vectors learned by word2vec for countries and their capitals [**?**].

will see how we use these vectors to replace the manually-designed features in our NLP applications.

8.5 Drawbacks of the Word2vec Algorithm

Word2vec has the same drawbacks as the low-rank approximation algorithm previously discussed. Both approaches produce vectors that suffer from lack of interpretability, although one could argue that word2vec's vectors are even less interpretable than the low-rank vectors in the $\mathbf{U}$ matrix, whose dimensions can be somewhat explained using the $\mathbf{V}^T$ matrix. Further, word2vec also conflates all senses of a given word into a single numerical representation. That is, the word *bank* gets a single numerical representation regardless of whether its current context indicates a financial sense, e.g., *Bank of America*, or a geological one, e.g., *bank of the river*. In Chapter 10 we will discuss strategies to build word vector representations that are sensitive of the current context in which a word appears.

8.6 Historical Background

TODO: todo

8.7 References and Further Readings

TODO: todo

9 Implementing the Neural Review Classifier Using Word Embeddings

10 Contextualized Embeddings and Transformer Networks

TODO: Transformer networks; BERT; BERT variants

11 Using Transformers with the Hugging Face Library

12 Sequence Models

TODO: CNNs, RNNs

13 Implementing Sequence Models in PyTorch

14 Sequence-to-sequence Methods

TODO: Seq2seq without and with attention

15 Domain Transfer

TODO: Mixing source and destination datasets; neural forms of Hal Daumé's frustratingly easy algorithm

16 Semi-supervised Learning and Other Advanced Topics

TODO: Traditional bootstrapping. One-shot algorithms, e.g., Valpola's mean teacher

Author’s Biography

Your Name

Your Name began life as a small child ...