Explaining the Success of Nearest Neighbor Methods in Prediction
**Other titles in Foundations and Trends® in Machine Learning**

*Non-convex Optimization for Machine Learning*
Prateek Jain and Purushottam Kar

*Kernel Mean Embedding of Distributions: A Review and Beyond*
Krikamol Muandet, Kenji Fukumizu, Bharath Sriperumbudur and Bernhard Schölkopf
ISBN: 978-1-68083-288-4

*Tensor Networks for Dimensionality Reduction and Large-scale Optimization: Part 1 Low-Rank Tensor Decompositions*
Andrzej Cichocki, Anh-Huy Phan, Qibin Zhao, Namgil Lee, Ivan Oseledets, Masashi Sugiyama and Danilo P. Mandic
ISBN: 978-1-68083-222-8

*Tensor Networks for Dimensionality Reduction and Large-scale Optimization: Part 2 Applications and Future Perspectives*
Andrzej Cichocki, Anh-Huy Phan, Qibin Zhao, Namgil Lee, Ivan Oseledets, Masashi Sugiyama and Danilo P. Mandic
ISBN: 978-1-68083-276-1

*Patterns of Scalable Bayesian Inference*
Elaine Angelino, Matthew James Johnson and Ryan P. Adams
ISBN: 978-1-68083-218-1

*Generalized Low Rank Models*
Madeleine Udell, Corinne Horn, Reza Zadeh and Stephen Boyd
Explaining the Success of Nearest Neighbor Methods in Prediction

George H. Chen
Carnegie Mellon University
georgechen@cmu.edu

Devavrat Shah
Massachusetts Institute of Technology
devavrat@mit.edu
Editorial Scope

Topics

Foundations and Trends® in Machine Learning publishes survey and tutorial articles in the following topics:

- Adaptive control and signal processing
- Applications and case studies
- Behavioral, cognitive and neural learning
- Bayesian learning
- Classification and prediction
- Clustering
- Data mining
- Dimensionality reduction
- Evaluation
- Game theoretic learning
- Graphical models
- Independent component analysis
- Inductive logic programming
- Kernel methods
- Markov chain Monte Carlo
- Model choice
- Nonparametric methods
- Online learning
- Optimization
- Reinforcement learning
- Relational learning
- Robustness
- Spectral methods
- Statistical learning theory
- Variational inference
- Visualization

Information for Librarians

Foundations and Trends® in Machine Learning, 2018, Volume 10, 6 issues. ISSN paper version 1935-8237. ISSN online version 1935-8245. Also available as a combined paper and online subscription.
Contents

1 Introduction 3
   1.1 Explaining the Popularity of Nearest Neighbor Methods 5
   1.2 Nearest Neighbor Methods in Theory 8
   1.3 The Scope of This Monograph 9

2 Background 13
   2.1 Regression 14
   2.2 Classification 17
   2.3 Nearest Neighbor and Kernel Regression 21
   2.4 Nearest Neighbor and Kernel Classification 24

3 Theory on Regression 26
   3.1 Overview of Results 27
   3.2 Key Definitions, Technicalities, and Assumptions 40
   3.3 Theoretical Guarantees for $k$-NN Regression 45
   3.4 Theoretical Guarantees for Fixed-Radius NN Regression 61
   3.5 Theoretical Guarantees for Kernel Regression 66
   3.6 Proofs 68
   3.7 Choice of Number of Nearest Neighbors and Kernel Bandwidth 100

4 Theory on Classification 105
   4.1 Converting Guarantees from Regression to Classification 108
Explaining the Success of Nearest Neighbor Methods in Prediction

George H. Chen¹ and Devavrat Shah²

¹Carnegie Mellon University; georgechen@cmu.edu
²Massachusetts Institute of Technology; devavrat@mit.edu

ABSTRACT

Many modern methods for prediction leverage nearest neighbor search to find past training examples most similar to a test example, an idea that dates back in text to at least the 11th century and has stood the test of time. This monograph aims to explain the success of these methods, both in theory, for which we cover foundational nonasymptotic statistical guarantees on nearest-neighbor-based regression and classification, and in practice, for which we gather prominent methods for approximate nearest neighbor search that have been essential to scaling prediction systems reliant on nearest neighbor analysis to handle massive datasets. Furthermore, we discuss connections to learning distances for use with nearest neighbor methods, including how random decision trees and ensemble methods learn nearest neighbor structure, as well as recent developments in crowdsourcing and graphons.

In terms of theory, our focus is on nonasymptotic statistical guarantees, which we state in the form of how many training data and what algorithm parameters ensure that a nearest neighbor prediction method achieves a user-specified error tolerance. We begin with the most general of such results.

for nearest neighbor and related kernel regression and classification in general metric spaces. In such settings in which we assume very little structure, what enables successful prediction is smoothness in the function being estimated for regression, and a low probability of landing near the decision boundary for classification. In practice, these conditions could be difficult to verify empirically for a real dataset. We then cover recent theoretical guarantees on nearest neighbor prediction in the three case studies of time series forecasting, recommending products to people over time, and delineating human organs in medical images by looking at image patches. In these case studies, clustering structure, which is easier to verify in data and more readily interpretable by practitioners, enables successful prediction.
1

Introduction

Things that appear similar are likely similar. For example, a baseball player’s future performance can be predicted by comparing the player to other similar players (Silver, 2003). When forecasting election results for a U.S. state, accounting for polling trends at similar states improves forecast accuracy (Silver, 2008). In image editing, when removing an object from an image, one of the most successful ways to fill in the deleted pixels is by completing the missing pixels using image patches similar to the ones near the missing pixels (Criminisi et al., 2004). These are but a few examples of how finding similar instances or nearest neighbors help produce predictions. Of course, this idea is hardly groundbreaking, with nearest neighbor classification already appearing as an explanation for visual object recognition in a medieval text Book of Optics by acclaimed scholar Alhazen in the early 11th century.\(^1\) Despite their simplicity and

\(^1\)A brief history of nearest neighbor classification and its appearance in Alhazen’s Book of Optics is given by Pelillo (2014). The exact completion date of Optics is unknown. Al-Khalili (2015) dates the work to be from years 1011 to 1021, coinciding with much of Alhazen’s decade of imprisonment in Cairo, while Smith (2001) claims a completion time between 1028 and 1038, closer to Alhazen’s death circa 1040.
Introduction

age, nearest neighbor methods remain extremely popular,\(^2\) often used as a critical cog in a larger prediction machine. In fact, the machine can be biological, as there is now evidence that fruit flies’ neural circuits execute approximate nearest neighbor in sensing odors as to come up with an appropriate behavioral response (Dasgupta et al., 2017).

Although nearest neighbor classification dates back a millennium, analysis for when and why it works did not begin until far more recently, starting with a pair of unpublished technical reports by Fix and Hodges (1951; 1952) on asymptotic convergence properties as well as a small dataset study, followed by the landmark result of Cover and Hart (1967) that showed that \(k\)-nearest neighbors classification achieves an error rate that is at most twice the best error rate achievable. Decades later, Cover recollected how his paper with Hart came about:

Early in 1966 when I first began teaching at Stanford, a student, Peter Hart, walked into my office with an interesting problem. He said that Charles Cole and he were using a pattern classification scheme which, for lack of a better word, they described as the nearest neighbor procedure. This scheme assigned to an as yet unclassified observation the classification of the nearest neighbor. Were there any good theoretical properties of this procedure? (Cover, 1982)

It would take some time for the term “nearest neighbor” to enter common parlance. However, the nearest neighbor procedure spread quickly across areas in computer science. Not long after Cover and Hart’s 1967 paper, Donald Knuth’s third volume of *The Art of Computer Programming* introduced nearest neighbor search as the *post office problem* (Knuth, 1973), paving the beginnings of computational geometry. In various coding theory contexts, *maximum likelihood decoding* turns out to mean nearest neighbor classification (Hill, 1986). Fast forwarding to present time, with the explosion in the availability of data in virtually all disciplines, architecting database systems that scale to this volume

\(^2\)Not only was the \(k\)-nearest neighbor method named as one of the top 10 algorithms in data mining (Wu et al., 2008), three of the other top 10 methods (AdaBoost, C4.5, and CART) have nearest neighbor interpretations.
1.1. Explaining the Popularity of Nearest Neighbor Methods

That nearest neighbor methods remain popular in practice largely has to do with their empirical success over the years. However, this explanation is perhaps overly simplistic. We highlight four aspects of nearest neighbor methods that we believe have been crucial to their continued popularity. First, the flexibility in choosing what “near” means in nearest neighbor prediction allows us to readily handle *ad-hoc* distances, or to take advantage of existing representation and distance learning machinery such as deep neural networks or decision-tree-based ensemble learning approaches. Second, the computational efficiency of numerous approximate nearest neighbor search procedures enables nearest neighbor prediction to scale to massive high-dimensional datasets common in modern applications. Third, nearest neighbor methods are nonparametric, making few modeling assumptions on data and instead letting the data more directly drive predictions. Lastly, nearest neighbor methods are interpretable: they provide evidence for their predictions by exhibiting the nearest neighbors found.

*Flexibility in defining similarity.* Specifying what “near” means for a nearest neighbor method amounts to choosing a “feature space” in which data are represented (as “feature vectors”), and a distance function to use within the feature space. For example, a common choice for the feature space and distance function are Euclidean space and Euclidean distance, respectively. Of course, far more elaborate choices are possible and, in practice, often these are chosen in an *ad-hoc* manner depending on the application. For example, when working with time series, the distance function could involve a highly nonlinear time warp (to try to align two time series as well as possible before computing a simpler distance like Euclidean distance). In choosing a “good” feature space (*i.e.*, a good way to *represent* data), features could be manually “hand-engineered” depending on the data modality (*e.g.*, text, images, video, audio) or...
learned, for example, using deep neural networks (e.g., Goodfellow et al. 2016, Chapter 15). Meanwhile, sensor fusion is readily possible as features extracted from multiple sensors (e.g., different data modalities) can be concatenated to form a large feature vector. Separately, the distance function itself can be learned, for example using Mahalanobis distance learning methods (Kulis, 2013) or Siamese networks (Bromley et al., 1994; Chopra et al., 2005). In fact, decision trees and their use in ensemble methods such as random forests, AdaBoost, and gradient boosting can be shown to be weighted nearest neighbor methods that learn a distance function (we discuss this relationship toward the end of the monograph in Section 7.1, building on a previous observation made by Lin and Jeon 2006). Thus, nearest neighbor methods actually mesh well with a number of existing representation and distance learning results.

**Computational efficiency.** Perhaps the aspect of nearest neighbor methods that has contributed the most to their popularity is their computational efficiency, which has enabled these methods to scale to massive datasets (“big data”). Depending on the feature space and distance function chosen or learned by the practitioner, different fast approximate nearest neighbor search algorithms are available. These search algorithms, both for general high-dimensional feature spaces (e.g., Gionis et al. 1999; Datar et al. 2004; Bawa et al. 2005; Andoni and Indyk 2008; Ailon and Chazelle 2009; Muja and Lowe 2009; Boytsov and Naidan 2013; Dasgupta and Sinha 2015; Mathy et al. 2015; Andoni et al. 2017) and specialized to image patches (e.g., Barnes et al. 2009; Ta et al. 2014), can rapidly determine which data points are close to each other while parallelizing across search queries. These methods often use locality-sensitive hashing (Indyk and Motwani, 1998), which comes with a theoretical guarantee on approximation accuracy, or randomized trees (e.g., Bawa et al. 2005; Muja and Lowe 2009; Dasgupta and Sinha 2015; Mathy et al. 2015), which quickly prune search spaces when the trees are sufficiently balanced. These randomized trees can even be efficiently constructed for streaming data using an arbitrary distance function (Mathy et al., 2015).
1.1. Explaining the Popularity of Nearest Neighbor Methods

Nonparametric. Roughly speaking, nearest neighbor methods being nonparametric means that they make very few assumptions on the underlying model for the data. This is a particularly attractive property since in a growing number of modern applications such as social networks, recommendation systems, healthcare decision support, and online education, we wish to analyze big data that we do not know the structure of. A nonparametric approach sidesteps the question of explicitly positing or learning the structure underlying the data. When we posit intricate structure for data, the structure may stray from reality or otherwise not account for the full palette of possibilities in what the data look like. When we learn structure, the computational overhead and amount of data needed may dwarf what is sufficient for tackling the prediction task at hand. Instead of positing or learning structure, nonparametric methods let the data more directly drive predictions. However, being nonparametric doesn’t mean that nearest neighbor methods have no parameters. We still have to choose a feature space and distance, and a poor choice of these could make prediction impossible.

Interpretability. Nearest neighbor methods naturally provide evidence for their decisions by exhibiting the nearest neighbors found in the data. A practitioner can use the nearest neighbors found to diagnose whether the feature space and distance function chosen are adequate for the application of interest. For example, if on validation data, a nearest neighbor method is making incorrect predictions, we can look at the nearest neighbors of each validation data point to see why they tend to have incorrect labels. This often gives clues to the practitioner as to how to choose a better feature space or distance function. Alternatively, if the nearest neighbor method is producing accurate predictions, the nearest neighbors found tell us which training data points are driving the prediction for any particular validation or test point. This interpretability is vital in applications such as healthcare that demand a high burden of proof before letting software influence potentially costly decisions that affect people’s well-being.
1.2 Nearest Neighbor Methods in Theory

Although nearest neighbor methods for prediction have remained popular, only recently has a thorough theory been developed to characterize the error rate of these methods in fairly general settings. Roughly a millennium after the appearance of nearest neighbor classification in Alhazen’s *Book of Optics*, Chaudhuri and Dasgupta (2014) established arguably the most general performance guarantee to date, stating how many training data and how to choose the number of nearest neighbors to achieve a user-specified error tolerance, when the data reside in a metric space. This flavor of result is “nonasymptotic” in that it can be phrased in a way that gives the probability of misclassification for any training data set size; we do not need an asymptotic assumption that the amount of training data goes to infinity. Chaudhuri and Dasgupta’s result subsumes or matches classical results by Fix and Hodges (1951), Devroye *et al.* (1994), Cérou and Guyader (2006), and Audibert and Tsybakov (2007), while providing a perhaps more intuitive explanation for when nearest neighbor classification works, accounting for the metric used and the distribution from which the data are sampled. Moreover, we show that their analysis can be translated to the regression setting, yielding theoretical guarantees that nearly match the best of existing regression results.

However, while the general theory for both nearest neighbor classification and regression has largely been fleshed out, a major criticism is that they do not give “user-friendly” error bounds that can readily be computed from available training data (Kontorovich and Weiss, 2015). For example, Chaudhuri and Dasgupta’s result for nearest neighbor classification depends on the probability of landing near the true decision boundary. Meanwhile, nearest neighbor regression results depend on smoothness of the function being estimated, usually in terms of Lipschitz or more generally Hölder continuity parameters. In practice,

---

3Within the same year a few months after Chaudhuri and Dasgupta’s paper appeared on arXiv, Gadat *et al.* posted on arXiv the most general theory to date for nearest neighbor classification in the more restricted setting of finite dimensional spaces, which was finally published two years later in *Annals of Statistics* (Gadat *et al.*, 2016).
these quantities are typically difficult to estimate for a real dataset. Unfortunately, this also makes the theory hard to use by practitioners, who often are interested in understanding how many training data they should acquire to achieve a certain level of accuracy, preferably in terms of interpretable application-specific structure rather than, for instance, Hölder continuity parameters (e.g., in healthcare, each training data point could correspond to a patient, and the cost of conducting a study may scale with the number of patients; being able to relate how many patients should be in the study in terms of specific disease or treatment quantities that clinicians can estimate would be beneficial).

Rather than providing results in as general a setting as possible, a recent trilogy of papers instead shows how clustering structure that is present in data enables nearest neighbor prediction to succeed at time series forecasting, recommending products to people, and finding human organs in medical images (Chen et al., 2013; Bresler et al., 2014; Chen et al., 2015). These papers establish nonasymptotic theoretical guarantees that trade off between the training data size and the prediction accuracy as a function of the number of clusters and the amount of noise present. The theory here depends on the clusters being separated enough so that noise is unlikely to cause too many points to appear to come from a wrong cluster. Prediction succeeds when, for a test point, its nearest neighbors found in the training data are predominantly from the same cluster as the test point. That these theoretical guarantees are about clustering is appealing because clusters can often be estimated from data and interpreted by practitioners.

1.3 The Scope of This Monograph

This monograph aims to explain the success of nearest neighbor methods in prediction, covering both theory and practice. Our exposition intentionally strives to be as accessible as possible to theoreticians and practitioners alike. As the number of prediction methods that rely on nearest neighbor analysis and the amount of literature studying these methods are both enormous, our coverage is carefully curated and inexhaustive.
Introduction

On the theoretical side, our goal is to provide some of the most general *nonasymptotic* results and give a flavor of the proof techniques involved. All key theoretical guarantees we cover are stated in the form of how many training data and what algorithm parameters ensure that a nearest neighbor prediction method achieves a user-specified error tolerance.

On the more practical side, we cover some examples of how nearest neighbor methods are used as part of a larger prediction system (recommending products to people in the problem of *online collaborative filtering*, and delineating where a human organ is in medical images in the problem of *patch-based image segmentation*). We also discuss a variety of approximate nearest neighbor search and related methods which have been pivotal to scaling nearest neighbor prediction to massive, even ever-growing datasets.

Our coverage is as follows, transitioning from theory to practice as we progress through the monograph:

- **Background (Chapter 2).** We anchor notation and terminology used throughout the monograph. Specifically we define the basic prediction tasks of classification and regression, and then present the three basic algorithms of $k$-nearest neighbor, fixed-radius near neighbor, and kernel regression. These regression methods can in turn be translated into classification methods.

- **Regression (Chapter 3).** We present theoretical guarantees for $k$-nearest neighbor, fixed-radius near neighbor, and kernel regression where the data reside in a metric space. The proofs borrow heavily from the work by Chaudhuri and Dasgupta (2014) with some influence from the work by Gadat *et al.* (2016). These authors actually focus on classification, but proof ideas translate over to the regression setting.

- **Classification (Chapter 4).** We show how the theoretical guarantees for regression can readily be converted to ones for classification. However, it turns out that we can obtain classification guarantees using weaker conditions. We explain how Chaudhuri...
and Dasgupta (2014) achieve this for \( k \)-nearest neighbor classification and how the basic idea readily generalizes to fixed-radius near neighbor and kernel classification.

- **Prediction Guarantees in Three Contemporary Applications (Chapter 5).** We present theoretical guarantees for nearest neighbor prediction in time series forecasting (Chen et al., 2013), online collaborative filtering (Bresler et al., 2014), and patch-based image segmentation (Chen et al., 2015). Despite these applications seeming disparate and unrelated, the theoretical guarantees for them turn out to be quite similar. In all three, clustering structure enables successful prediction. We remark that the independence assumptions on training data and where clustering structure appears are both application-specific.

- **Computation (Chapter 6).** We provide an overview of efficient data structures for exact and approximate nearest neighbor search that are used in practice. We focus on motifs these methods share rather than expounding on theoretical guarantees, which many of these methods lack. Our starting point is the classical \( k \)-\( d \) tree data structure for exact nearest neighbor search (Bentley, 1979), which works extremely well for low-dimensional data but suffers from the “curse of dimensionality” due to an exponential dependence on dimension when executing a search query. To handle exact high-dimensional nearest neighbor search, more recent approaches such as the cover tree data structure exploit the idea that high-dimensional data often have low-dimensional structure (Beygelzimer et al., 2006). As such approaches can still be computationally expensive in practice, we turn toward approximate nearest neighbor search. We describe locality-sensitive hashing (LSH) (Indyk and Motwani, 1998), which forms the foundation of many approximate nearest neighbor search methods that come with theoretical guarantees. We also discuss empirically successful approaches with partial or no theoretical guarantees: random projection or partition trees inspired by \( k \)-\( d \) trees, and the recently proposed boundary forest.
• **Adaptive Nearest Neighbors and Far Away Neighbors** *(Chapter 7).* We end with remarks on distance learning with a focus on decision trees and various ensemble methods that turn out to be nearest neighbor methods, and then turn toward a new class of nearest neighbor methods that in some sense can take advantage of far away neighbors.

For readers seeking a more “theory-forward” exposition albeit without coverage of Chaudhuri and Dasgupta’s classification and related regression results, there are recent books by Devroye *et al.* *(2013)* (on classification) and Biau and Devroye *(2015)* (on nearest neighbor methods with sparse discussion on kernel regression and classification), and earlier books by Györfi *et al.* *(2002)* (on nonparametric regression) and Tsybakov *(2009)* (on nonparametric estimation). Unlike the other books mentioned, Tsybakov’s regression coverage emphasizes fixed design (corresponding to the training feature vectors having a deterministic structure, such as being evenly spaced in a feature space), which is beyond the scope of this monograph. As for theory on nearest neighbor search algorithms, there is a survey by Clarkson *(2006)* that goes into substantially more detail than our overview in Chapter 6. However, this survey does not cover a number of very recent advances in approximate nearest neighbor search that we discuss.
References


Full text available at: http://dx.doi.org/10.1561/2200000064
References


Chaudhuri, K. and S. Dasgupta (2014). “Rates of convergence for nearest neighbor classification”. In: Advances in Neural Information Processing Systems. 3437–3445. The different versions of this paper have different numberings for theorems, equations, etc. The numbering we use is from arXiv: 1407.0067v2 [cs.LG].


References


Full text available at: http://dx.doi.org/10.1561/2200000064


References


Full text available at: http://dx.doi.org/10.1561/2200000064


