Random projections: data perturbation for classification problems

Citation for published version:

Digital Object Identifier (DOI):
10.1002/wics.1499

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Early version, also known as pre-print

Published In:
Wiley Interdisciplinary Reviews: Computational Statistics

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Random projections: data perturbation for classification problems

Timothy I. Cannings
School of Mathematics, University of Edinburgh

Abstract

Random projections offer an appealing and flexible approach to a wide range of large-scale statistical problems. They are particularly useful in high-dimensional settings, where we have many covariates recorded for each observation. In classification problems there are two general techniques using random projections. The first involves many projections in an ensemble – the idea here is to aggregate the results after applying different random projections, with the aim of achieving superior statistical accuracy. The second class of methods include hashing and sketching techniques, which are straightforward ways to reduce the complexity of a problem, perhaps therefore with a huge computational saving, while approximately preserving the statistical efficiency.

Figure 1: Projections determine distributions! Left: two 2-dimensional distributions, one uniform on the unit circle (black), the other uniform on the unit disk (blue). Right: the corresponding densities after the projecting into a 1-dimensional space. In fact, any $p$-dimensional distribution is determined by its one-dimensional projections (cf. Theorem 1).
1 INTRODUCTION

Modern approaches to data analysis go far beyond what early statisticians, such as Ronald A. Fisher, may have dreamt up. Rapid advances in the way we can collect, store and process data, as well as the value in what we can learn from data, has led to a vast number of innovative and creative new methods.

Broadly speaking, random projections offer a universal and flexible approach to complex statistical problems. They are a particularly useful tool in large-scale settings, such as high-dimensional classification (Durrant and Kabán, 2013, 2015; Cannings and Samworth, 2017), clustering (Dasgupta, 1999; Fern and Brodley, 2013; Heckel et al., 2017), precision matrix estimation (Marzetta et al., 2011), regression (Klanke et al., 2008; McWilliams et al., 2014; Heinze et al., 2016; Thanei et al., 2017, 2018; Slawska, 2018; Dobriban and Liu, 2019), sparse principal component analysis (Gataric et al., 2019), hypothesis testing (Lopes et al., 2011; Shi et al., 2019), correlation estimation (Grellman et al., 2016), dimension reduction (Bingham and Mannilla, 2001; Reeve et al., 2017) and matrix decomposition (Halko et al., 2011).

Random projections are an example of a data perturbation technique. In general, data perturbation refers to an approach in which one does not apply a method directly to the raw data set, but rather looks at a perturbed version (or perhaps many perturbed versions) of the data. This idea has a long history: perhaps the most well-known example is the Bootstrap. Since Efron coined the term in his seminal 1979 paper (Efron, 1979), the Bootstrap has been extensively studied and developed – it has received multiple book-length treatments, e.g. Efron and Tibshirani (1993), Shao and Tu (1995) and Davison and Hinkley (1997); see also the more recent paper Kleiner et al. (2014) on large-scale applications of the Bootstrap. The Bootstrap works by recalculating many statistics based on different random subsamples (with replacement) of the observations, with the aim of understanding the uncertainty of an estimator.

In prediction problems, bootstrap aggregation, or bagging (Breiman, 1996a), can be used to improve the accuracy of a simple method. By aggregating the results of many predictions based on bootstrapped predictions, one can obtain a final accurate prediction with low variance. See, for instance, Hall and Samworth (2005), Biau and Devroye (2010), Biau et al. (2010) and Samworth (2012) who study the properties of the bagged nearest neighbour classifier. The extremely popular random forests algorithm, neatly combines bagging with classification and regression trees (Breiman et al., 1984; Breiman, 2001).

Other, more recent data perturbation techniques include stability selection (Meinshausen and Bühlmann, 2010; Shah and Samworth, 2013), which is designed to improve the performance of a variable selection algorithm by aggregating the results of applying a base selection procedure to many subsamples of the data. Shah and Meinshausen (2014) propose a related method called random intersection trees, which aims to find interactions between
the variables in high-dimensional problems. The knockoff filter (Barber and Candès, 2015) guarantees control of the false discovery rate in a variable selection problem, by constructing exchangeable “knockoff” copies of the features that are independent of the response – if a variable is not selected before its knockoff copy it is likely to be a false discovery. Finally, Hinton et al. (2012) propose a data perturbation method called dropout, which aims to prevent a neural network from overfitting – see also Wager et al. (2013).

The remainder of this paper focusses on random projection methods in classification problems. Classification is one of the fundamental problems in statistical learning. In the simple, binary version, we are presented with the task of assigning a test observation to one of two classes, based on a number of training observations from each class. This problem dates back at least to the aforementioned Fisher, who applied his Linear Discriminant Analysis (LDA) method to identify the species of Iris plants based on measurements of the petal and sepal sizes (Fisher, 1936). Modern applications are seemingly endless; think, for instance, of a spam filter sorting email into the appropriate folders; a driverless car determining whether a hazard is approaching; a doctor classifying tumours in an x-ray; or a smart-watch recognising the wearers activity and adding one (or not) to their step-count for the day.

Classification has been studied by statisticians, computer scientists, machine learners and AI researchers. The basic methods include, among hundreds of others, linear discriminant analysis (LDA), its quadratic counterpart (QDA), \( k \)-nearest neighbours (\( \text{knn} \)) (Fix and Hodges, 1951), support vector machines (SVM) (Cortes and Vapnik, 1995), trees and random forests (Breiman et al., 1984; Breiman, 2001), empirical risk minimisation (ERM) (Vapnik, 1992), kernel methods (Marron, 1983) and neural networks and deep learners (LeCun et al., 2015). Further discussion of these techniques and many others can be found in, for example, Devroye et al. (1996), Boucheron et al. (2005) and Hastie et al. (2009).

A common theme in modern applications is the size of the datasets involved – we often have a huge amount of data. The term high-dimensional refers to a situation where the number of features \( p \) is comparable to or larger than (perhaps much larger than) the total number of observations \( n \). This setting typically leads to problems for existing methods – the so-called curse of dimensionality. Either we lose statistical accuracy (Bickel and Levina, 2004) or suffer a prohibitive computational cost. In fact, some methods are simply intractable in high-dimensional settings, for example LDA requires the inverse of a sample covariance matrix, which will be singular if \( p > n \); see also Wainwright (2019, Example 1.2.1).

Recently, there have been a number of proposals aimed at dealing with high-dimensional data in a classification problem – see, for examples, Friedman (1989), Hastie et al. (1995), Tibshirani et al. (2002), Tibshirani et al. (2003), Fan and Fan (2008), Witten and Tibshirani (2011) and Fan et al. (2012). It is typically assumed in these works that the optimal decision boundary is linear, and only a small proportion of the features are relevant for classification.
In this article, we see that random projections offer an alternative solution to high-dimensional classification problems. The use of random projections is motivated by two fundamental results. The first is that a distribution is determined by its one-dimensional projections – a result sometimes referred to as the Cramér–Wold device.

**Theorem 1.** Suppose \( X_1 \) and \( X_2 \) are independent random vectors taking values in \( \mathbb{R}^p \). Fix \( d \in \{1, \ldots, p\} \). If \( AX_1 = d AX_2 \) for every \( A \in \mathbb{R}^{d \times p} \), then \( X_1 = d X_2 \).

The proof of this result is very simple using characteristic functions: For \( t \in \mathbb{R}^p \), there exists \( s \in \mathbb{R}^d \) and \( A \in \mathbb{R}^{d \times p} \) such that \( t = A^T s \). Thus

\[
\mathbb{E}\{\exp(it^T X_1)\} = \mathbb{E}\{\exp(is^T AX_1)\} = \mathbb{E}\{\exp(is^T AX_2)\} = \mathbb{E}\{\exp(it^T X_2)\}.
\]

Heuristically speaking, therefore, we can learn a high-dimensional distribution by looking only at its low-dimensional projections.

Our second motivating result is the Johnson–Lindenstrauss Lemma. This states that a set of arbitrary points in a high-dimensional ambient space can be mapped into a low-dimensional space, while approximately preserving the pairwise distances between the points. We state the result in a form relating directly to random projections.

**Theorem 2.** Let \( \epsilon, \delta > 0 \), and for \( n \geq 2 \), suppose that \( x_1, \ldots, x_n \) are distinct vectors in \( \mathbb{R}^p \). Fix \( d > \frac{16 \log(n/\delta)}{\epsilon^2} \), and let \( A \) be a random projection taking values in \( \mathbb{R}^{d \times p} \) with independent \( N(0, 1/p) \) entries. Then, with probability greater than \( 1 - \delta \), we have

\[
1 - \epsilon < \frac{\|Ax_i - Ax_j\|^2}{\|x_i - x_j\|^2} < 1 + \epsilon, \quad \text{for every } i \neq j \in \{1, \ldots, n\}.
\]

The proof of the Johnson–Lindenstrauss Lemma is based on the concentration of \( \chi^2 \) random variables; more details can be found in, for example, Dasgupta and Gupta (2002), Ailon and Chazelle (2006) and Wainwright (2019, Example 2.12). The power of this result is perhaps quite striking: notice that the lower bound on the projected dimension \( d \) does not depend on the ambient dimension \( p \), and scales only logarithmically in the number of data points \( n \). Suppose, for instance, that we have 1000 observations in one million dimensions – a scale often seen in modern applications – let \( \epsilon = 0.1 \) and \( \delta = 0.01 \), then the lower bound on \( d \) is around 18000. In other words, using just one random projection of the data, we can reduce the dimension by a number of orders of magnitude, while potentially almost preserving the statistical efficiency.

Many authors have sought to simplify the random projections used in the Johnson–Lindenstrauss Lemma (Achlioptas, 2003; Li et al., 2006; Le et al., 2013). Moreover, Larsen and Nelson (2016) showed that the lower bound on \( d \) is optimal.
The remainder of this paper will focus on two approaches to using random projections in classification. The first we will call ensemble methods (cf. Section 3), which typically seek to improve the statistical accuracy of a method, by applying it to many random projections of the data. The second, which will be referred to as sketching (cf. Section 4), looks to improve the computational efficiency of an algorithm by first reducing the effective sample size or data dimension using a random projection, with the hope that one does not lose out in terms of statistical accuracy. We then conclude the paper with a number of discussion points and open problems. First, in the next section, we introduce the statistical framework used throughout the paper.

2 STATISTICAL SETTING

Let \((X,Y), (X_1,Y_1), \ldots, (X_n,Y_n)\), be independent and identically distributed pairs, taking values in \(\mathbb{R}^p \times \{0,1\}\), with distribution \(P\). We observe the training data \(T_n = \{(X_1,Y_1), \ldots, (X_n,Y_n)\}\), the test point \(X\) and would like to predict the class \(Y\). Here \(n\) and \(p\) will be referred to as the sample size and (ambient) dimension, respectively. We can characterise the joint distribution \(P\) by fixing the marginal \(X\) distribution \(P_X\) and specifying the regression function \(\eta(x) := \mathbb{P}(Y = 1 | X = x)\); alternatively, we can fix the marginal \(Y\) distribution by specifying prior probabilities \(\pi_1 := \mathbb{P}(Y = 1) = 1 - \mathbb{P}(Y = 0) =: 1 - \pi_0\), and then generate \(X\) according to the class-conditional distribution \(X|\{Y = r\} \sim P_r\), for \(r = 0,1\).

A classifier is a (measurable) function \(C : \mathbb{R}^p \to \{0,1\}\), with the interpretation that the point \(x \in \mathbb{R}^p\) is assigned to the class \(C(x)\). It is useful to let \(\mathcal{C}_p\) denote the space of all \(p\)-dimensional classifiers. In practice, we construct classifiers based on the training data \(T_n\), which we will typically denote by \(C_n : (\mathbb{R}^p \times \{0,1\})^\otimes n \to \mathcal{C}_p\). In other words, \(C_n\) is a rule (or algorithm) that constructs a classifier in \(\mathcal{C}_p\) depending on the training data \(T_n\).

We often seek classifiers with low test (or misclassification) error

\[
R(C) := \int_{\mathbb{R}^p \times \{0,1\}} 1_{\{C(x) \neq y\}} \, dP(x,y).
\]

We write the test error as an integral here to make it clear that we are only averaging over the distribution of the test pair \((X,Y)\). The test error is minimised by the Bayes classifier

\[
C_{\text{Bayes}}(x) := \begin{cases} 
1 & \text{if } \eta(x) \geq 1/2 \\
0 & \text{otherwise};
\end{cases}
\]

see, for instance, Devroye et al. (1996, Theorem 2.1). We have that \(R(C_{\text{Bayes}}) = \mathbb{E}[\min\{\eta(X), 1 - \eta(X)\}]\).
In what follows, we will construct classifiers using the (random) training data as well as random projections. In order to keep track of the different sources of randomness, random projections will be displayed in bold (typically by \textbf{A}, \textbf{A}_1, etc.). Fixed, non-random projections will be presented in plain typeface, i.e. \textit{A}, \textit{A}_1, etc.. We use \textit{E} and \textit{P} to denote expectation and probability, respectively, taken over the randomness of the projections (conditionally on the training data). On the other hand, \textit{E} and \textit{P} are used to refer to expectation and probability, respectively, over all sources of randomness (i.e. random training data, the random test point, and the random projections). We will use the convention that \textit{A} and \textit{A} will take values in \( \mathbb{R}^{d \times p} \), and will therefore map a point \( x \in \mathbb{R}^p \) to \( Ax \in \mathbb{R}^d \). Finally, the term \textit{Gaussian random projection} will be used to refer to a projection with independent \( N(0, 1/p) \) entries, a \textit{Haar} projection is one uniformly distributed on the set \( \{ A \in \mathbb{R}^{d \times p} : AA^T = I_{d \times d} \} \), whereas an \textit{axis-aligned} projection has orthonormal rows and one non-zero entry equal to 1 in each row.

3 ENSEMBLE METHODS

Ensemble methods work by aggregating many (typically randomised) estimators. The intuition is that combining the results of many noisy but unbiased predictions will lead to an unbiased prediction with low variance. The aforementioned bagging procedure is perhaps the most widely used ensemble approach in classification. As noted by Breiman\(^1\) “\textit{bagging can push a good but unstable procedure towards optimality. On the other hand, it can slightly degrade the performance of stable procedures}”. A similar statement can be made about some methods based on random projections.

Early empirical work demonstrated the potential power of random projection ensembles: Schclar and Rokach (2009) showed that a simple majority vote random projection ensemble classifier was competitive with bagging in some settings. In the remainder of this section, we provide an overview of some recent random projection based ensemble methods, with a particular aim to summarise the associated theoretical guarantees.

3.1 The random-projection ensemble classifier

The \textit{random-projection ensemble classifier}, proposed in a recent paper by Cannings and Samworth (2017), works by aggregating the results of applying an arbitrary base classifier to many carefully chosen low-dimensional random projections of the data. It can be seen “\textit{as a general technique for either extending the applicability of an existing method to high}

\(^1\)Breiman (1996a, p. 124)
dimensions, or simply improving its performance”\textsuperscript{2}.

Figure 2: Different two-dimensional projections of 200 observations in \( p = 50 \) dimensions. 
Top row: three projections drawn from Haar measure; bottom row: the projections with the smallest estimate of test error out of 100 Haar projections for the LDA (left), QDA (middle) and \( knn \) (right) base classifiers. Reproduced with permission from Cannings and Samworth (2017, Fig. 1).

One of the key observations is that aggregating the results of applying all the projections is not effective – indeed, most (low-dimensional) random projections in the high-dimensional setting lead to a random guess – see Figure 2. Cannings and Samworth (2017) instead therefore advocate selecting good projections based on an estimate of the test error after applying each one. A second key observation is that combining the results via a simple majority vote is typically not suitable – indeed the intuition one might have from bagging no longer applies – the random-projection ensemble classifier instead uses a biased majority vote, with a data-driven voting threshold.

The random-projection ensemble classifier is given in Algorithm 1. We first formally define some notation used in the construction of the classifier. Let \( d \leq p \) (one should think of \( d \) being small, \( \leq 10 \), say), and assume we have a base classifier \( C_{n,d} = C_{n,T_{n,d}} \), which can be constructed from any training sample \( T_{n,d} \) of size \( n \) in \( \mathbb{R}^d \times \{0,1\} \); thus \( C_{n,d} \) is a

\textsuperscript{2}Cannings and Samworth (2017, p. 961)
measurable function from \((\mathbb{R}^d \times \{0, 1\})^n \times \mathbb{R}^d\) to \(\{0, 1\}\). Given a projection \(A \in \mathbb{R}^{d \times p}\), let \(\mathcal{T}_n^A := \{(AX_1, Y_1), \ldots, (AX_n, Y_n)\}\). The projected data base classifier corresponding to \(C_{n,d}\) is \(C_n^A : (\mathbb{R}^d \times \{0, 1\})^n \times \mathbb{R}^p \to \{0, 1\}\), given by

\[ C_n^A(x) = C_{n, \mathcal{T}_n^A}(x) := C_{n, \mathcal{T}_n^A}(Ax). \]

Note that although \(C_n^A\) is a classifier on \(\mathbb{R}^p\), the value of \(C_n^A(x)\) only depends on \(x\) through its \(d\)-dimensional projection \(Ax\). Now, let \(R_n^A\) be an estimator of the test error \(R(C_n^A)\) based on \(\mathcal{T}_n^A\). Examples of such estimators include the training error and leave-one-out estimator; see Cannings and Samworth (2017, Section 4) for more detail.

**Algorithm 1: The random-projection ensemble classifier**

**Result:** \(C_{n}^{\text{RP}}(x) = \mathbbm{1}_{\{\nu_{B_1}^{B_1}(x) \geq \alpha\}}\)

**Data:** \(\mathcal{T}_n\) and the test point \(x \in \mathbb{R}^p\)

**Input:** \(\alpha \in [0, 1], B_1, B_2, d \in \mathbb{N}\), a projected data base classifier \(C_{n,d}\);

**for** \(b_1 = 1, \ldots, B_1\) **do**

**for** \(b_2 = 1, \ldots, B_2\) **do**

- Generate a Gaussian projection \(A_{b_1,b_2}\);
- Project the training data to give \(\mathcal{T}_n^{A_{b_1,b_2}}\);
- Estimate \(R(C_{n}^{A_{b_1,b_2}})\) by \(R_n^{A_{b_1,b_2}}\);

**end**

Set \(A_{b_1} = A_{b_1}^{b_2}(b_1)\), where \(b_2^{*}(b_1) := \operatorname{sargmin}_{b_2 = 1, \ldots, B_2} \left\{ R_n^{A_{b_1,b_2}} \right\}\);

**end**

Let \(\nu_{B_1}^{B_1}(x) := \frac{1}{B_1} \sum_{b_1=1}^{B_1} \mathbbm{1}_{\{C_{n}^{A_{b_1}}(x) = 1\}}\).

Notice the flexibility offered by the framework in Algorithm 1. The practitioner may use their favourite base classifier (Cannings and Samworth (2017) study the LDA, QDA and \(k\)nn base classifiers in detail), any projection distribution and any way of measuring the performance of a projection. Details of how to choose \(\alpha\) depending on the training data are given in (Cannings and Samworth, 2017, Section 5.2). The method can be implemented using the \texttt{RPEnsemble} (Cannings and Samworth, 2016) package available from CRAN.

The construction in Algorithm 1 means that the chosen projections \(A_1, \ldots, A_{B_1}\) depend on the training data, but are in fact conditionally independent given the training data. This allows for theoretical analysis. Indeed, Cannings and Samworth (2017, Theorem 1) studies the performance of the algorithm as \(B_1\) increases; it is shown that the error of an ensemble using \(B_1\) random projections converges to the error of the infinite ensemble at rate \(B_1^{-1}\) – thus one should choose \(B_1\) as large as possible up to a computational constraint – see Figure 3 for a numerical demonstration of this.
Figure 3: The average error (black) plus/minus two standard deviations (red) of $C_{\text{RP}}^n$ over 20 sets of $B_1B_2$ projections for $B_1 \in \{2, \ldots, 500\}$ and $B_2 = 50$. The plots show the test error for one training dataset for the LDA (left), QDA (middle) and $k$nn (right) projected data base classifiers. Reproduced with permission from Cannings and Samworth (2017, Fig. 2).

The choice of $B_2$ is less straightforward due to potential issue of overfitting (Cannings and Samworth, 2017, Theorem 3). If $B_2$ is too small, then we may only be averaging over noise (cf. Figure 2). On the other hand if $B_2$ is too large, then we may select a set of projections that are good for the training data, but do not generalise well. From a practical viewpoint, the default choices of $d = 5$, $B_1 = 500$ and $B_2 = 50$ typically work very well (cf. Section 3.3). Another main theoretical contribution in Cannings and Samworth (2017) is that, under a low-dimensional structure assumption, the average performance of the random-projection ensemble classifier may be bounded by terms that do not depend on the ambient dimension $p$ (cf. Cannings and Samworth (2017, Theorem 3 and Proposition 2)). More precisely, the assumption is as follows: for a projection $A$ and $z \in \mathbb{R}^d$, let $\eta^A(z) := \mathbb{P}(Y = 1 | AX = z)$. Now, suppose that there exists a projection $A^* \in \mathbb{R}^{d \times p}$, for which

$$P_X\{x \in \mathbb{R}^p : \eta(x) \geq 1/2\} \Delta\{x \in \mathbb{R}^p : \eta^{A^*}(A^* x) \geq 1/2\} = 0, \quad (1)$$

where $B \Delta C = (B \cap C^c) \cup (B^c \cap C)$ denotes the symmetric difference of two sets $B$ and $C$ (cf. Cannings and Samworth (2017, Assumption 3)). This condition can be seen as a generalisation of those typically used in the high-dimensional classification literature: if the Bayes decision boundary is linear, then (1) holds with $d = 1$; under the common sparse signal assumption that only $d$ of the features are relevant for classification, (1) holds with an axis-aligned choice of $A^*$; finally, (1) holds under the sufficient dimension reduction assumption that $Y$ is conditionally independent of $X$ given $A^*X$ (Cook, 1998).

The computational cost of the random-projection ensemble classifier is discussed in Cannings and Samworth (2017, Section 5.1). One of the appealing features of the method is its compatibility with parallel computing – we can simultaneously compute the projected data
base classifier for each of the $B_1 B_2$ projections.

There was a stimulating and constructive discussion of the paper. A number of method-
ological variations were proposed. These included how to generate the random projections,
to subsequently assess each projection’s performance, and then how to aggregate the results.
The original paper focussed on Haar and Gaussian distributed projections. Alternatives
include using axis-aligned projections, which are well-suited to the ultrahigh-dimensional
setting, or very sparse random projections (Li et al., 2006) – see also Mylavarapu and Kabán
(2013) for a direct comparison of random projections versus random feature selection. An-
other suggestion was to sequentially update the projections, attempting to improve the
predictions each time. While intuitively appealing, Cannings and Samworth (2017) found
that, in fact, (as observed by Breiman) having a diverse set of projections is desirable – some
discussants even suggested to enforce some orthogonality constraint. Typically, however, in
high dimensions two projections chosen as described in Algorithm 1 are close to orthogonal
anyway.

Other discussants suggested alternative ways to aggregate the results. Many proposed a
weighted combination similar to that used in boosting (Freund and Schapire, 1996, 1999); or
to use a blending/stacking method (Wolpert, 1992; Breiman, 1996b), which involves applying
a classifier that uses the predictions from the base classifiers themselves as new features.

Blaser and Fryzlewicz (2015) investigate a related method using random rotations as
opposed to projections. In their work a classifier suited to high-dimensional data is applied
after each rotation. In a follow up paper, Blaser and Fryzlewicz (2019) advocate selecting
good rotations based on their complexity, where simpler learners are preferred. Gul et al.
(2016) propose an ensemble method based on applying the $k$-nearest neighbour classifier to
subsamples of the training data – they randomly choose subsets of both the features and
the observations. This process is repeated many times and the top performing projections
(measured on an out-of-bag sample) are retained. The results of applying the $knn$ classifier
with the chosen samples are then combined to construct the final classifier. Khan et al.
of randomly chosen linear base classifiers, and provide a bound on the performance of their
method based on the VC-dimension. They show empirically that it is competitive with
random kitchen sinks (Rahimi and Recht, 2007) and Adaboost (Freund and Schapire, 1999).

There is also some recent general theoretical work on understanding ensemble methods.
Lopes (2019b) derives the rate at which the test error of a finite ensemble approaches its
infinite simulation counterpart. Lopes (2019a) proposes a bootstrap method to approximate
the variance of an ensemble, with a view to ascertain how large an ensemble is needed.

In summary, the random-projection ensemble classifier offers a general approach to high-
dimensional statistical problems. At a high level, just three key ingredients are required: (i)
a suitable low-dimensional method for the problem at hand; (ii) a measure of the relative performance after applying each projection; and (iii) an effective aggregation procedure. Gataric et al. (2019) introduce a new method for sparse principal component analysis based on this framework – in their work, the target is to obtain a low-dimensional projection of the data that explains the greatest proportion of the population variance. Since the components in the projection are assumed to be sparse, it is preferable to use axis-aligned projections, as opposed to Gaussian projections. Very recently, Anderlucci et al. (2019) applied this framework in the unsupervised clustering problem, where a Gaussian mixture model assumption is used in order to assess the quality of each projection, and a technique known as consensus clustering is used to aggregate the results.

3.2 Model based ensembles

Other works have exploited the use random projections to directly estimate the model parameters in a high-dimensional classification problem. This is the setting investigated in Durrant and Kabán (2015) (see also Marzetta et al. (2011)), where multiple random projections of the data are used to estimate the high-dimensional precision matrix in LDA.

Suppose, for simplicity, that $X|\{Y = r\} \sim N_p(\mu_r, \Sigma)$, for $r = 0, 1$, where $\mu_0, \mu_1 \in \mathbb{R}^p$, and $\Sigma$ is a $p \times p$ covariance matrix common to both classes. The Bayes classifier in this case is

$$C_{\text{LDA-Bayes}}(x) = \begin{cases} 1 & \text{if } \log\left(\frac{\pi_1}{\pi_0}\right) + (x - \frac{\mu_1 + \mu_0}{2})^T \Sigma^{-1}(\mu_1 - \mu_0) \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$  \hspace{1cm} (2)$$

Its risk can be expressed in terms of $\pi_0, \pi_1$, and the squared Mahalanobis distance $\Delta^2 = (\mu_1 - \mu_0)^T \Sigma^{-1}(\mu_1 - \mu_0)$ between the classes

$$R(C_{\text{LDA-Bayes}}) = \pi_0 \Phi\left(\frac{1}{\Delta} \log\left(\frac{\pi_1}{\pi_0}\right) - \frac{\Delta}{2}\right) + \pi_1 \Phi\left(\frac{1}{\Delta} \log\left(\frac{\pi_0}{\pi_1}\right) - \frac{\Delta}{2}\right),$$

where $\Phi$ denotes the standard normal distribution function.

The LDA classifier is constructed by substituting training data estimates of $\pi_0, \pi_1, \mu_0, \mu_1, \Sigma$ into (2). These are given by $\hat{\pi}_r = \frac{1}{n} \sum_{i=1}^n \mathbb{1}_{\{Y_i = r\}}$, $\hat{\mu}_r = \frac{1}{n_r} \sum_{i=1}^{n_r} X_i \mathbb{1}_{\{Y_i = r\}}$, and

$$\hat{\Sigma} = \frac{1}{n - 2} \sum_{i=1}^n \sum_{r=0}^1 (X_i - \hat{\mu}_r)(X_i - \hat{\mu}_r)^T \mathbb{1}_{\{Y_i = r\}}.$$ 

As mentioned in the introduction, if $p > n$, then $\hat{\Sigma}$ will be singular, and LDA is intractable in its vanilla form.

Durrant and Kabán (2015) advocate estimating $\Sigma$ using random projections. For $B \in \mathbb{N}$, let $A_1, \ldots, A_B$ be independent Gaussian random projections taking values in $\mathbb{R}^{d \times p}$. Then
let

\[
C_n^{\text{LDA-Ens}}(x) = \begin{cases} 
1 & \text{if } \log\left(\frac{n_1}{n_0}\right) + \frac{1}{B} \sum_{b=1}^{B}(x - \frac{\hat{\mu}_1 + \hat{\mu}_0}{2})^T A_b^T (A_b \hat{\Sigma} A_b^T)^{-1} A_b (\hat{\mu}_1 - \hat{\mu}_0) \geq 0 \\
0 & \text{otherwise.}
\end{cases}
\]

In other words, the ensemble uses \( \hat{\Sigma}_B^{-1} = \frac{1}{B} \sum_{b=1}^{B} A_b^T (A_b \hat{\Sigma} A_b^T)^{-1} A_b \) as an estimate of \( \Sigma^{-1} \).

Note that the terms in the sum \( A_b \hat{\Sigma} A_b^T \) are invertible almost surely as long as \( d < \min\{n, p\} \).

Durrant and Kabán (2015, Theorem 3.2) derive a bound on the test error of an LDA classifier that uses the converged ensemble precision matrix \( E(\hat{\Sigma}_B^{-1}) \). The bound depends on how well \( E(\hat{\Sigma}_B^{-1}) \) approximates \( \Sigma^{-1} \), as well as the squared Mahalonobis distance \( \Delta \) and the balance between the two class sizes. The accuracy of the precision matrix estimate itself \( \hat{\Sigma}_B^{-1} \) (with finite \( B \)) was further investigated in Kabán (2017).

### 3.3 The epileptic seizure recognition data set

We now demonstrate the utility of the methods described in this section with a brief numerical study. The epileptic seizure recognition data set (Andrzejak et al., 2001) available from the UCI Machine Learning repository\(^3\) contains 11500 observations of a 179-dimensional EEG recording. Associated with each observation is a label in \( \{1, \ldots, 5\} \) corresponding to whether the patient was experiencing an epileptic seizure or not. We simplify the problem by combining the four “no seizure” classes, so that the task is to predict \( Y \in \{0, 1\} \), where class 0 and class 1 correspond to “no seizure” and “seizure”, respectively. In the resulting dataset, there are 9200 observations in class 0 and 2300 in class 1.

To assess the performance of the classifiers, we take a random sample of size 1000 to use as a test set (this remains fixed throughout the study) and our experiments are repeated 100 times on different (randomly chosen) training samples. There are two studies: one with \( n = 100 \) and one with \( n = 1000 \). We compare seven classifiers: (vanilla) LDA, (vanilla) QDA, two based on \( C_n^{\text{LDA-Ens}} \), and the random-projection ensemble classifier with three different choices of base classifiers. For \( C_n^{\text{LDA-Ens}} \), we set \( d = \frac{1}{2} \min\{n - 2, p\} \) as recommended in Durrant and Kabán (2015), and we use an ensemble of \( B = 1000 \) Gaussian random projections (LDA_1000) – for comparison we also include the results when just one projection is used (LDA_1). For the random-projection ensemble classifiers, we use the LDA, QDA, and \( k \)nn base methods and the default parameters recommended in Cannings and Samworth (2017), that is \( d = 5 \), \( B_1 = 500 \) and \( B_2 = 50 \). The voting cutoff \( \alpha \) was chosen using

\(^3\)https://archive.ics.uci.edu/ml/datasets/Epileptic+Seizure+Recognition
the method described in Cannings and Samworth (2017, Section 5.2). These methods are denoted by \( \text{RP}_\text{LDA} \), \( \text{RP}_\text{QDA} \) and \( \text{RP}_\text{knn} \) in Figure 4.

![Figure 4: The estimated test errors for the experiments described in Section 3.3 using the epileptic seizure recognition data set. Left panel: \( n = 100 \). Right panel: \( n = 1000 \).](image)

In Figure 4 we present boxplots of the test errors for the 100 repetitions of each experiment. First note that, for \( n = 100 \), the LDA and QDA classifiers are intractable since \( n < p \). In fact, for \( n = 1000 \), there are 5 out of the 100 experiments where QDA is still intractable, since there were fewer than 179 observations in the minority class in those cases. We see that the LDA ensemble method of Durrant and Kabán (2015) offers a tractable version of the LDA classifier, but it is not particularly effective in this problem. The random-projection ensemble classifier with the QDA base classifier is very accurate for both sample sizes and the \( \text{knn} \) base classifier gives the best results when \( n = 1000 \).

## 4 SKETCHING AND HASHING

The aim of sketching and hashing is to reduce the complexity of a problem, by reducing the (effective) sample size or dimension, respectively, while approximately preserving the statistical efficiency. These techniques can often lead to a huge computational saving – in fact, in some cases, we may not have sufficient disk space to store the raw data, and therefore some form of sketching may be required. In contrast to the previous section on ensemble methods, typically only one projection or sketch is used to train the classifier.

Perhaps the simplest random sketching approach is to subsample the observations – suppose, for example, that we have a huge number of observations (\( 10^6 \), say), but are interested in a straightforward problem, such as LDA. If the data dimension is low, then we will perhaps obtain sufficiently accurate results with around 1000 observations; including the full dataset
in the estimation of the parameters in LDA will only give minor improvements. As a result we do not need to store the full dataset, and our estimation procedure will be much faster. With this approach the data dimension is unchanged and it is unlikely to be successful if \( p \) is large. Of course, with a large amount of data available, it is also likely that a more sophisticated approach than LDA will be possible.

Other works have investigated sketching techniques that involve premultiplying the \( n \times p \) data matrix \((X_1, \ldots, X_n)^T\) and the \( n \times 1 \) vector of responses (or classes) \((Y_1, \ldots, Y_n)^T\) by a random \( \Omega \in \mathbb{R}^{m \times n} \) projection. Again, like subsampling, the dimension of the problem stays the same, but the effective sample size may be reduced significantly. This technique has received a fair amount of attention in the context of kernel ridge regression (Yang et al., 2017; Avron et al., 2017; Dobriban and Liu, 2019), but comparatively little in classification problems.

There are a number of works that advocate applying an existing classifier after projecting the features into a lower dimensional space. Typically, the idea in these problems is to reduce the dimension, and thus the computational cost, while preserving performance guarantees using an argument similar to the Johnson–Lindenstrauss Lemma (cf. Theorem 2). Note that, in contrast to Section 3.1, where low-dimensional projections were used (i.e. \( d \leq 10 \)), for the Johnson–Lindenstrauss Lemma to be effective, the projection dimension should grow with the logarithm of the sample size \( n \). For instance, it is often shown that under some condition on the dimension of the image space of the map that, with high-probability (over the randomness in the projection), the error of the classifier trained on the projected data is close to that which could be obtained by training the classifier in the ambient high-dimensional space.

This approach has been studied in combination with Fisher’s linear discriminant analysis (Durrant and Kabán, 2010, 2012; Elkhali et al., 2019; Skubalska-Rafałowicz, 2019). Recall the class-conditional Gaussian setting introduced in Section 3.2. Let \( A \) be a Gaussian random projection and define

\[
C_n^{\text{LDA}}(x) = \begin{cases} 
1 & \text{if } \log \left( \frac{\hat{\pi}_1}{\hat{\pi}_0} \right) + \left( x - \frac{\hat{\mu}_1 + \hat{\mu}_0}{2} \right)^T A \left( A \Sigma A^T \right)^{-1} A (\hat{\mu}_1 - \hat{\mu}_0) \geq 0 \\
0 & \text{otherwise.}
\end{cases}
\]

Durrant and Kabán (2012, Theorem 4.8) provide a bound on the average (over the projection) test error of \( C_n^{\text{LDA}} \). A similar result was shown in Durrant and Kabán (2013) for a classifier based on linear empirical risk minimisation. One of the key aspects of these works is the so-called flipping probability (Durrant and Kabán, 2013, Theorem 3.2), which specifies the chance that the label assigned to a point in the ambient \( p \)-dimensional is “flipped” (from zero to one or vice-versa) after applying a random projection.

Other works in this direction focus on alternative base methods, for instance, the \( k \)-nearest neighbour classifier (Ailon and Chazelle, 2006; Kabán, 2015; Reeve and Brown, 2017)
and support vector machines (Rahimi and Recht, 2007; Paul et al., 2012). Xie et al. (2016) investigate combining random projection techniques with other dimension reduction methods, such as principal component analysis.

In some settings it is in fact possible to exactly encode a high-dimensional dataset via a low-dimensional representation. Indeed, suppose that the feature vectors are high-dimensional, binary and sparse – i.e. $X$ takes values in $\{0, 1\}^p$, but only a small proportion of the features are non-zero for each observation. Shah and Meinshausen (2018) propose an approach to large scale classification and regression in this context, based on $b$-bit min-wise hashing (Li and Köng, 2011). They show how the min-wise hashing technique can be combined with logistic regression in order to give improved computational and statistical efficiency.

Finally, we mention that some hashing and sketching techniques are designed to guarantee privacy – by applying a non-invertable map (or projection) to the data, we can ensure that any sensitive information is hidden – for some examples in this direction, see Kenthapadi et al. (2013) and Upadhyay (2013).

5 DISCUSSION

Despite the large body of work mentioned in this review, the use of random projections in classification problems (and indeed in wider statistical problems) is perhaps still in its early stages. A number of practical considerations remain. Perhaps at the forefront of those are general concerns about randomised methods – for instance, two different practitioners may obtain different results using the same method, simply by using different initial randomisation seeds. That being said, ensemble approaches partially derandomise procedures, and the huge popularity of methods like random forests suggests that practitioners are often happy to overlook this issue.

Many random projection based approaches are so-called black box methods – they may classify accurately, but offer limited interpretation as to how a decision was made. In some applications this is not an issue. Think, for example, of an email spam filter, where, if an email is designated to the spam folder, we’re not interested in why that decision was made. On the other hand, suppose a doctor is using a randomised algorithm to help diagnose a disease, it is of limited practical use if the classifier simply produces a yes or no answer (unless it is perfectly accurate).

One way to aid interpretability is to provide a relative ranking of the importance of each of the features in the model. There is some numerical work in this direction, for instance, Breiman (2001, Section 10) proposes a variable importance measure for the random forest algorithm. Moreover, for the random-projection ensemble classifier, the chosen pro-
jections provide a natural way of ranking the features. There is, however, relatively little understanding of the precise theoretical properties of such approaches.

Further considerations include testing the robustness of such methods – what if the data is noisy or missing? There has been a fair amount of work recently on label noise (Frénay & Kabán, 2014; Frénay & Verleysen, 2014). Simple methods such as k-nearest neighbours and support vector machines have been shown to be robust to label noise (Cannings et al., 2019). It is less clear, however, how more sophisticated methods, such as those based on random projections, will be affected by noise.

There are many other open questions remaining on the use of random projections in statistics. First, there are computational and statistical trade-offs that are not precisely understood. How about optimality – what can be learnt (in a minimax sense) from random projections of the data? Finally, while a distribution is determined by the distributions of its projections (cf. Theorem 1), and we perhaps have a good understanding of how well we can approximate the low-dimensional distributions from projected data, it is not understood how this translates to learning the properties of the high-dimensional distribution.

References


**FURTHER READING**

**General topics**


**The knockoff filter**


**Large-scale optimisation**


**Random kernel expansions**

