Robust Linear Discriminant Analysis Using Tyler's Estimator: Asymptotic Performance Characterization


Published in:
IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP’19)

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2019 IEEE. This work is made available online in accordance with the publisher’s policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal 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 Research Portal is Queen’s institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Download date: 27. Mar. 2022
We consider a robust version of regularized discriminant analysis (RDA) classifiers to account for potential spurious or mislabeled observations in the training data set. To build a robust discriminant rule, a robust estimation of the covariance matrix is essential. In this work, we propose to use a regularized version of Tyler’s covariance estimator, in the regime where both the number of variables and the number of training samples are large and of similar order. Building upon fundamental results from random matrix theory, we show that the robust classifier is asymptotically equivalent to traditional, non-robust classifiers when the training data is free from outliers. Simulations on synthetic and real datasets confirm our theoretical observations and further attest to the benefits brought by the robust classifier when the data is corrupted by outliers.

Index Terms— Robust estimation, covariance matrices, linear discriminant analysis

1. INTRODUCTION

Discriminant analysis is a common classification method used in statistics, machine learning, and pattern recognition to identify the combination of features that best separate a number of classes of events or objects [1]. Discriminant analysis belongs to the wide class of parametric classification methods [2], which assume that the data follows a certain distribution (for example, a Gaussian mixture model). Based on labeled data, from which estimates of the class means and covariance matrices are obtained, a discrimination rule is learned, which is then used to determine the class which an unseen data sample most likely pertains to.

When dealing with real data sets, it is often the case that the number of variables is of the same order as (or even larger than) the number of available samples. In such cases, classical estimators of covariance matrices like the sample covariance matrix (SCM) typically fail. To solve this issue, regularized versions of discriminant analysis have been proposed [3], based on regularized versions of the SCM. Regularized discriminant analysis has since then established itself as the go-to choice in practice. In a series of recent works [4, 5], RDA has been studied from a random matrix theory perspective. Specifically, when the number of variables and the number of samples grow large at the same rate, an asymptotic equivalent of the classification error has been found, shedding some light on the influence of the data model on the performance of RDA.

A common problem arising in discriminant analysis is the fact that the data, although assumed to arise from a Gaussian mixture model, is often not Gaussian: data samples may instead follow a heavy-tailed distribution, or some of the training samples may be outliers, the origin of which can be diverse (for a review, see [6]). This is a critical issue in practice; as the discriminant rule learned from the training data necessitates the estimation of the covariance matrix of the data, when outliers are present and/or if the data is not Gaussian, using a simple estimate like the sample covariance matrix can lead to underwhelming results. It is then natural to aim for a robust estimation of the covariance matrix. In this work, we consider a regularized version of Tyler’s estimator of covariance, proposed in [7, 8], and we study the asymptotic performance of the associated discriminant rule in the context of linear discriminant analysis (LDA). To do so, we build on a series of recent works concerned with the performance analysis of RDA [4, 5] and the asymptotic behavior of Tyler’s estimator [9, 10]. We first demonstrate that, when no outliers are present in the data, there is no performance loss when using regularized Tyler’s estimator rather than the regularized SCM (RSCM). We then validate this observation with simulations on synthetic data and on the MNIST dataset. It is also shown empirically that, when the data is corrupted by a certain type of outliers, there is a clear benefit in using this robust estimator rather than the RSCM.

Notation: The superscript $^T$ means transpose. $tr\mathbf{A}$ represents the trace of the matrix $\mathbf{A}$. $||.||$ denotes the Euclidean norm for vectors and the spectral norm for matrices. $\Phi(\cdot)$ denotes the cumulative density function of the standard normal distribution. The arrow $\overset{a.s.}{\longrightarrow}$ designates the almost sure convergence of a random variable.

2. DISCRIMINANT ANALYSIS

2.1. Model

In discriminant analysis, a discriminant rule is determined so as to decide to which class a given (unseen) data vector most likely belongs. Such rule is built based on an available training data set composed of $n$ samples pertaining to, say, $2$ classes, $C_0, C_1$. Assume that the $n_t > 0$ observations from
class $C_i$ are independent and sampled from a multivariate Gaussian distribution with mean $\mu_i \in \mathbb{R}^{N \times 1}$ and covariance matrix $\Sigma \in \mathbb{R}^{N \times N}$, with $\Sigma \succeq 0$.

The linear discriminant rule consists in assigning a new (test) measurement $x$ to class $C_k$ if
\[
k = \arg \min_{i \in \{0,1\}} \left\{ (x - \mu_i)^T \Sigma^{-1} (x - \mu_i) - \log \pi_i \right\}, \tag{1}\]

with $\pi_i(n) \triangleq n_i/n$ the a priori probability of class $C_i$. The LDA rule therefore assigns the label 0 to observation $x$ if $P(x|x \in C_0) > P(x|x \in C_1)$, and the label 1 otherwise.

Since the true means $\mu_i$ and the population matrix $\Sigma$ appearing in the LDA rule are unknown, in practice they need to be estimated based on the training data $\{x(i)_j \in C_i, \ i = 0,1, \ j = 1, \cdots, n_i\}$. Possible estimates for $\mu_i, \Sigma$ are the sample estimates
\[
\hat{x}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} x(i)_j, \quad i \in \{0,1\}
\]
\[
\hat{S} = \frac{1}{n-2} \left( (n_0-1) \hat{S}_0 + (n_1-1) \hat{S}_1 \right) ,
\]
where
\[
\hat{S}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} (x(i)_j - \hat{x}_i) (x(i)_j - \hat{x}_i)^T , \quad i \in \{0,1\}.
\]

The estimator $\hat{S}$ is usually referred to as the “pooled SCM” in the literature. The main issue with these sample estimates is that they are known to perform poorly when the number of samples is of the same order as the number of variables (or possibly smaller). In practice, to alleviate the potential ill-conditioning of the sample covariance matrix, a regularized estimator, referred to as RSCM, is typically used [3]
\[
\Sigma(\rho) = I_N + \rho \hat{S} . \tag{2}
\]

2.2. Classification error of linear discriminant analysis
Let $\hat{H}$ be an estimator of $\Sigma^{-1}$. Then, conditioned on the training data $x_1, \cdots, x_n$, the probability of misclassification is given by [4]
\[
\epsilon_i^{\text{LDA}}(\hat{H}) = e_i^{(n)} c_i^{\text{LDA}}(\hat{H}) + \pi_i^{(n)} c_i^{\text{LDA}}(\hat{H}) \tag{3}
\]
with $e_i^{(n)}(\hat{H})$, $i \in \{0,1\}$, the class-conditional classification error verifying
\[
e_i^{\text{LDA}}(\hat{H}) = \Phi \frac{(-1)^{i+1} G(\hat{H}) + (-1)^i \log \pi_i^{(n)}}{\sqrt{D(\hat{H})}} , \tag{4}
\]
where
\[
G(\hat{H}) = \left( \mu_i - \hat{x}_0 + \hat{x}_1 \right)^T \hat{H} (\hat{x}_0 - \hat{x}_1) ,
\]
\[
D(\hat{H}) = (\hat{x}_0 - \hat{x}_1)^T \hat{H} \Sigma \hat{H} (\hat{x}_0 - \hat{x}_1) . \tag{5}
\]

An issue with standard RDA is that it is not robust if outlying samples are present in the training data. In such cases, of much practical relevance, we can resort to a robust covariance estimator, as discussed next.

3. ROBUST LDA IN CLEAN DATA
3.1. Robust estimation of the covariance matrix
We propose to use a robust estimator of $\Sigma$ known as regularized Tyler’s estimator, defined as the unique solution $C(\beta)$ to the following fixed-point equation [7, 8]:
\[
C(\beta) = \frac{(1 - \beta)}{n - 2} \sum_{i=0}^{n} \sum_{j=1}^{n_i} \frac{(x(i)_j - \hat{x}_i) (x(i)_j - \hat{x}_i)^T}{\rho_{ij}^{(n)} H^{i-1}(\beta) (x(i)_j - \hat{x}_i)^T + \beta I_N} , \tag{6}
\]

where $\beta \in \{\max\{0,1 - n/N\}, 1\}$. This covariance matrix estimator is a hybrid estimator reminiscent of the original Tyler’s estimator of scale [11] and Ledoit-Wolf shrinkage estimator [12]. Here, like $\rho$ in the case of the RSCM (2), $\beta$ is a regularization parameter that determines the tradeoff between bias (the shrinkage target, $I_N$) and variance (the pooled SCM). Using the inverse of $C(\beta)$ as a plug-in estimator of $\Sigma^{-1}$ in (1), we should effectively end up with a robust version of LDA, which we coin Tyler-LDA. We note that, in [13], the authors also proposed to estimate the population matrix $\Sigma$ using regularized M-estimators (although excluding Tyler’s estimator) in the context of discriminant analysis, but did not provide a systematic analysis of the performance of their method.

An important question that naturally arises is whether Tyler-LDA performs (at least) as well as standard LDA approaches when the data is clean. This will be answered in the next section.

3.2. Asymptotic performance of Tyler-LDA
We operate under the following assumptions [5]:
Assumption 1. $N/n \triangleq c_N \to c \in (0, \infty)$ and $n_i/n \to \pi_i \in (0, \infty), \ i \in \{0,1\}$, as $n \to \infty$.

Assumption 2. $||\Sigma|| = O(1)$, and $||\mu|| = O(1)$, where $\mu \triangleq \mu_0 - \mu_1$.

Assumption 1 characterizes the growth regime under consideration, while Assumption 2, which is concerned with the covariance and mean scaling of the training data, ensures that a non-trivial (i.e., neither 0 or 1) asymptotic classification accuracy can be achieved [5].

In [4, 5], the authors studied the asymptotic performance (in terms of the total classification error) of the RSCM (2). In particular, they showed that, under Assumptions 1-2, the class-conditional classification error of the RSCM,
\[
e_i^{\text{RSCM}}(\rho) \triangleq \epsilon_i^{\text{LDA}}(\Sigma^{-1}(\rho))\]
converges to the deterministic quantity $\epsilon_i^{\text{RSCM}}(\rho)$, in the sense
\[
|\epsilon_i^{\text{RSCM}}(\rho) - \epsilon_i^{\text{RSCM}}(\rho)| \overset{a.s.}{\to} 0 , \quad N \to \infty,
\]
with $\epsilon_i^{\text{RSCM}}(\rho)$ depending only on the true means of each class and the underlying covariance matrix. The specifics of this result are recalled in Lemma 1, in Appendix.

As we will show, the asymptotic misclassification probability of Tyler-LDA is exactly the same as that of the RSCM when the training data is free of outliers. To proceed, let us define the asymptotic class-conditional classification error of
Tyler-LDA as $\hat{c}_i^{\text{Tyler}}(\beta) \triangleq \hat{c}_i^{\text{LDA}}(\beta \hat{C}^{-1}(\beta))$. Equipped with these assumptions and notations, we can now state our main result (proved in Section 5):

**Theorem 1.** [Deterministic equivalent] Let Assumptions 1-2 hold. For a given $\beta \in \mathcal{R}_C \triangleq [\zeta + \max\{0, 1 - c^{-1}\}, 1]$, where $\zeta \in (0, \min\{1, c^{-1}\})$, define $\rho_{\beta} = \frac{1}{\beta |(\beta - 1) - (1 - \beta)c|}$, where $\gamma(\beta)$ is the unique positive solution to the equation

$$
\frac{1}{N} \text{Tr}(\gamma(\beta) \beta I_N + (1 - \beta) \Sigma)^{-1} = 1.
$$

Then, $|\hat{c}_i^{\text{Tyler}}(\beta) - \hat{c}_i^{\text{Tyler}}(\beta)| \xrightarrow{a.s.} 0$ for each $\beta \in \mathcal{R}_C$, as $N, n \to \infty$, with $\hat{c}_i^{\text{Tyler}}(\beta) \triangleq \hat{c}_i^{\text{RSCM}}(\rho_{\beta})$, \hspace{1cm} (8)

with the expression of $\hat{c}_i^{\text{RSCM}}$ recalled in Lemma 1.

Theorem 1 shows that, when data is outlier-free, both the standard regularized LDA method and Tyler-LDA share the same asymptotic performance, up to a transformation of the regularizer parameters. This is an important message, as it shows that there is nothing to lose by using Tyler’s estimator over other conventional methods when there are no outlying observations in the training data.

**Regularization parameter optimization.** Among possible choices of $\beta \in \mathcal{R}_C$, in practice one shall choose the regularization parameter that minimizes the misclassification error $\hat{c}_i^{\text{Tyler}}(\beta)$. To do so, one can first use the optimization procedure proposed in [5] to find the optimal $\rho^*$ minimizing $\hat{c}_i^{\text{RSCM}}(\rho)$, and then use the inverse of the mapping $\beta \mapsto \rho$ given in Theorem 1 to identify a parameter $\beta^*$ that minimizes $\hat{c}_i^{\text{Tyler}}(\beta)$\hspace{1cm} (1). It then remains to estimate this (unknown) parameter based on the training sample. We will give more precise details in an extended version of the paper.

4. SIMULATIONS
4.1. Synthetic data
In all simulations, we used the sample mean as the mean estimator for $\mu_0$ and $\mu_1$. In Fig. 1, we plot the empirical classification error associated with the RSCM and Tyler’s estimator as a function of the regularization parameters $\rho$ and $\beta$ (top and bottom x-axes, respectively), in an outlier-free scenario. The deterministic classification error, computed using Theorem 1 and Lemma 1, and $\hat{c}_i^{\text{LDA}}(H = \Sigma)$ (“oracle” estimator) are also shown. Simulations show a very good match between empirical and theoretical values, which validates Theorem 1. We note that the optimal regularization parameters $\beta^*$ (for Tyler’s estimator) and $\rho^*$ (for the RSCM), identified on the figure, verify $\rho^* = \rho_{\beta^*}$ per the mapping given in the theorem statement.

Now consider a toy-example scenario where outliers (distributed as $\mathcal{N}(5\mu, I_N)$) are introduced in the training sample. To simplify the discussion, we fix $\rho = \rho^*$ and $\beta = \beta^*$, i.e., the optimal regularization parameters in the outlier-free case (setting of Fig. 1). Fig. 2 shows the classification error of both estimators as the proportion of outliers increases. It appears that outliers affect the performance of the RSCM more than that of Tyler’s estimator, with up to a 6% difference in misclassification probability when the data has only 5% outliers. This shows that, when data is corrupted by such outliers, Tyler’s estimator prevails over the RSCM, and it suggests that using Tyler’s estimator would be preferable over standard, non-robust methods when little is known about the quality of the training data.

**Fig. 1:** Classification error of the RSCM and Tyler’s estimator as $\rho$ and $\beta$ vary (top and bottom x-axes, respectively), for $N = 100$, $n_0 = n_1 = 200$, averaged over 1000 realizations, with a test sample size of 5000 samples per class. $\Sigma$ is such that $[\Sigma]_{ij} = 0.8^{\|i-j\|}$, and has eigenvalue decomposition $\Sigma = \mathbf{V}\Delta\mathbf{V}^T$. $\mu$ is such that $\mu \propto V1_{N}$. The oracle estimator’s classification error ($\Sigma$ assumed to be known) is also shown.

**Fig. 2:** Classification error of the RSCM and Tyler’s estimator, for $N = 100$, $n_0 = n_1 = 200$ (c/N = 1/4), averaged over 1000 realizations. Outliers follow a multivariate Gaussian distribution $\mathcal{N}(5\mu, I_N)$.

4.2. MNIST data
We also performed simulations on the MNIST data set [14]. For all 45 possible pairs of classes $C_0/C_1$ corresponding to digits 0/1, 0/2, ... etc., we computed the RSCM and Tyler’s estimator on all the available training data set ($\sim$5800 samples per class) and tested it on the testing data set ($\sim$1000
samples per class). Fig. 3 shows the statistics (as box plots) of the minimal testing classification error results for both estimators and all class pairs, obtained after a sweep over possible regularization parameters \( \rho \) and \( \beta \). Note that this provides a lower bound of the lowest classification error achievable on the given testing set, ignoring any effects of estimating the regularization parameter. The performance on some representative class pairs is also reported.

![Fig. 3: Box plot of the classification error of the RSCM and Tyler-LDA for all class pairs of the MNIST dataset (left), and comparison of the classification error for some specific class pair examples (right).](image)

We observe that the RSCM and Tyler’s estimator perform similarly (with a slight advantage, although non-statistically significant, for Tyler’s estimator), which appears consistent with our analysis, if one were to assume that the MNIST data is free of outliers. In practice, one should however estimate the optimal regularization parameter based on training data. To do so, the procedure briefly described in Subsection 3.2 can be used. As indicated, precise details on this shall be given in an extended version of this paper. It also remains to study the theoretical performance of the RSCM and of Tyler’s estimator under less clean scenarios; for example, with samples from different classes having different variances, or with outlying samples coming from a different distribution. This problem is currently under investigation.

5. PROOF OF THEOREM 1

The proof relies on understanding the asymptotic behavior of bilinear forms of the type \( a^T \hat{C}^{-k} \hat{C}^{-1} b \) \((k = 1, 2, \beta \in \mathcal{R}_\zeta)\), which appear in the expressions of \( G(\beta \hat{C}(\beta)^{-1}) \) and \( \hat{D}(\beta \hat{C}(\beta)^{-1}) \) in (5) and (6), used to compute the classification error \( e_t^{\text{Tyler}}(\beta) = e_t^{\text{LDA}}(\beta \hat{C}(\beta)^{-1}) \) in (4). This type of functional of \( \hat{C}^{-k} \hat{C}^{-1} \) is intricate, because \( \hat{C}(\beta) \) is only implicitly defined. However, along similar lines to the proof of [10, Lemma 3], it can be proved that for \( \beta \in \mathcal{R}_\zeta = \{ \zeta + \max\{0, 1 - e^{-1}\} \}, \) where \( \zeta \in (0, \min\{1, e^{-1}\}) \),

\[
\| \hat{C}(\beta) / \hat{C}^{-1} \| \xrightarrow{a.s.} 0, \quad n, N \to \infty, \tag{9}
\]

with \( \rho_\beta \) defined in Theorem 1. From this, it can be shown that the bilinear forms \( \beta^k a^T \hat{C}^{-k} \hat{C}^{-1} b \) are asymptotically close to their RSCM counterparts \( a^T \hat{\Sigma}(\rho_\beta)^{-k} b \), the behavior of which is well-understood. Specifically, for a given \( \beta \in \mathcal{R}_\zeta \), for \( a, b \in \mathbb{R}^N \) such that \( \lim_{n \to \infty} \| a \| < \infty \) a.s., \( \lim_{n \to \infty} \| b \| < \infty \) a.s., and \( k = 1, 2, \)

\[
\left| \beta^k a^T \hat{C}^{-k} \hat{C}^{-1} b - a^T \hat{\Sigma}(\rho_\beta)^{-k} b \right| \xrightarrow{a.s.} 0, \tag{10}
\]

as \( N, n \to \infty \). Taking for example \( k = 1 \), it is proved by first noting

\[
\left| a^T (\beta \hat{C}^{-1} - \hat{\Sigma}^{-1}(\rho_\beta) b) \right| \leq K \| \beta \hat{C}^{-1} - \hat{\Sigma}^{-1}(\rho_\beta) \| \leq K \cdot \| \hat{C}^{-1}(\beta) - \hat{\Sigma}^{-1}(\rho_\beta) \| \cdot \| \hat{\Sigma}(\beta)/\beta - \hat{\Sigma}(\rho_\beta) \|,
\]

where the last inequality is due to the resolvent identity [15], and where \( K = \| a \| / \| b \| \). The fact that \( \beta, \rho_\beta > 0 \) ensure that \( \| \hat{C}^{-1}(\beta) \| / \| \hat{\Sigma}^{-1}(\rho_\beta) \| < \infty \), which, along with (9) and \( \lim_{n \to \infty} \| a \| < \infty \) a.s., \( \lim_{n \to \infty} \| b \| < \infty \) a.s., leads to (10), for \( k = 1 \). The case \( k = 2 \) is handled similarly.

Equipped with this, we can prove that

\[
| G(\beta \hat{C}(\beta)^{-1}) - G(\hat{\Sigma}^{-1}(\rho_\beta)) | \xrightarrow{a.s.} 0 \tag{11}
\]

\[
| \hat{D}(\beta \hat{C}(\beta)^{-1}) - \hat{D}(\hat{\Sigma}^{-1}(\rho_\beta)) | \xrightarrow{a.s.} 0. \tag{12}
\]

Take \( a = \mu_i - (x_0 + x_1)/2 \) and \( b = (x_0 - x_1) \). Then, Assumption 2 implies \( \lim_{n \to \infty} \| a \| < \infty \) a.s., \( \lim_{n \to \infty} \| b \| < \infty \) a.s., by the law of large numbers. The convergence in (11) then follows from (10) by taking \( k = 1 \). For (12), we remark that

\[
| D(\beta \hat{C}(\beta)^{-1}) - \hat{D}(\hat{\Sigma}^{-1}(\rho_\beta)) | = | \hat{D}(\beta \hat{C}(\beta)^{-1}) - \hat{D}(\hat{\Sigma}^{-1}(\rho_\beta)) | \leq \| \hat{\Sigma} \| \cdot \| \hat{\Sigma}^{-1} - \hat{\Sigma}^{-2} \| \| b \| \| a \| \| b \|.
\]

Using (10) with \( k = 2 \) leads to (12).

From (4), using (11), (12), and the fact that \( \sqrt{\zeta} \) and \( \Phi(\cdot) \) are continuous functions, we have proved

\[
| e_t^{\text{Tyler}}(\beta) - e_t^{\text{RSCM}}(\rho_\beta) | \xrightarrow{a.s.} 0, \quad n, N \to \infty. \tag{13}
\]

Combining this with Lemma 1 concludes the proof.
References


