Efficient Learning of Minimax Risk Classifiers in High Dimensions

Karthikey Bondugula
Santiago Mazuelas
Aritz Pérez

1Basque Center for Applied Mathematics (BCAM), Bilbao, Spain
2IKERBASQUE-Basque Foundation for Science

Abstract

High-dimensional data is common in multiple areas, such as health care and genomics, where the number of features can be tens of thousands. In such scenarios, the large number of features often leads to inefficient learning. Constraint generation methods have recently enabled efficient learning of L1-regularized support vector machines (SVMs). In this paper, we leverage such methods to obtain an efficient learning algorithm for the recently proposed minimax risk classifiers (MRCs). The proposed iterative algorithm also provides a sequence of worst-case error probabilities and performs feature selection. Experiments on multiple high-dimensional datasets show that the proposed algorithm is efficient in high-dimensional scenarios. In addition, the worst-case error probability provides useful information about the classifier performance, and the features selected by the algorithm are competitive with the state-of-the-art.

1 INTRODUCTION

High-dimensional data is common in multiple areas such as health care and genomics. A typical example of high-dimensional supervised classification problem in genomics is to separate healthy patients from cancer patients based on gene expression data with tens of thousands of features [Guyon et al., 2002]. In addition to high-dimensional raw data, learning methods often perform a high-dimensional representation of the input data vector in order to improve the classification performance [Sonnenburg et al., 2006; Rahimi and Recht, 2008; Liu et al., 2017]. Learning in such high-dimensional settings often leads to highly complex optimization processes because the number of variables involved in the optimization increases with the number of features [Shi et al., 2010; Yuan et al., 2012].

In addition to high-dimensional data, a limited number of samples is common in the above-mentioned applications e.g., tens of thousands of features but less than 100 patients [Guyon and Elisseeff, 2003; Brown et al., 2012]. In such scenarios, the conventional performance assessment based on cross-validation can be unreliable [Varoquaux, 2018; Vabalas et al., 2019]. In addition, these cross-validation estimates also increase the computational cost as they require learning multiple classifiers.

Multiple methods have been proposed to improve the learning efficiency in high dimensions (see e.g., Yuan et al. (2012)). These methods are based on several approaches such as coordinate descent [Hsieh et al., 2008; Yu et al., 2011], interior-point method [Koh et al., 2007], and stochastic subgradient [Shalev-Shwartz et al., 2007]. In addition, multiple classification and regression methods exploit the parameters’ sparsity induced by convex penalties and regularization terms in high-dimensional settings [Mignacco et al., 2020; Celentano and Montanari, 2022]. Recently, constraint generation techniques have enabled the efficient learning of L1-regularized support vector machines (SVMs) for cases with a large number of features [Dedieu et al., 2022]. These techniques obtain improved efficiency for the linear program (LP) corresponding with binary L1-SVMs due to the sparsity in the solution.

In this paper, we present a learning algorithm for the recently proposed minimax risk classifiers (MRCs) [Mazuelas et al., 2020, 2023]. The presented algorithm provides efficient learning in high dimensions, obtains worst-case error probabilities that can serve to assess performance, and performs feature selection. Specifically, the main contributions in the paper are as follows.

- We present a learning algorithm for MRCs that utilizes constraint generation methods to significantly improve the efficiency in high dimensions.
- The presented algorithm utilizes a greedy feature selection approach that achieves a fast decrease in worst-case error probability while using a small number of features.
Our theoretical results show that the proposed algorithm obtains a sequence of classifiers with decreasing worst-case error probabilities that converges to the solution obtained using all the features.

Using multiple benchmark datasets, we experimentally show that the proposed algorithm performs efficient learning in high-dimensional settings. In addition, the algorithm obtains an error assessment for the classifier and performs effective feature selection.

Notations: For a set $S$, we denote its complement as $S^c$ and its cardinality as $|S|$; bold lowercase and uppercase letters represent vectors and matrices, respectively; vectors subscripted by a set of indices represent subvectors obtained by the components corresponding to the indices in the set; matrices subscripted by a set of indices represent submatrices obtained by the columns corresponding to the indices in the set; $\mathbf{I}$ denotes the identity matrix; $\mathbf{1}\{\cdot\}$ denotes the indicator function; $\mathbf{1}$ denotes a vector of ones; for a vector $\mathbf{v}$, $|\mathbf{v}|$ and $(\mathbf{v})_+$ denote its component-wise absolute value and positive part, respectively; $\|\cdot\|_1$ denotes the 1-norm of its argument; $\otimes$ denotes the Kronecker product; $\preceq$ and $\succeq$ denote vector inequalities; $\mathbb{E}_p\{\cdot\}$ denotes the expectation of its argument with respect to distribution $p$; and $e_i$ denotes the $i$-th vector in a standard basis.

2 PRELIMINARIES

In this section, we describe the setting addressed in the paper and MRC methods that minimize the worst-case error probability.

2.1 PROBLEM FORMULATION

Supervised classification uses instance-label pairs to determine classification rules that assign labels to instances. We denote by $\mathcal{X}$ and $\mathcal{Y}$ the sets of instances and labels, respectively, with $\mathcal{Y}$ represented by $\{1, 2, \ldots, |\mathcal{Y}|\}$. We denote by $T(\mathcal{X}, \mathcal{Y})$ the set of all classification rules (both randomized and deterministic) and we denote by $h(y|x)$ the probability with which rule $h \in T(\mathcal{X}, \mathcal{Y})$ assigns label $y \in \mathcal{Y}$ to instance $x \in \mathcal{X}$ ($h(y|x) \in \{0, 1\}$ for deterministic classification rules). In addition, we denote by $\Delta(\mathcal{X} \times \mathcal{Y})$ the set of probability distributions on $\mathcal{X} \times \mathcal{Y}$ and by $\ell(h, p)$ the expected 0-1 loss of the classification rule $h \in T(\mathcal{X}, \mathcal{Y})$ with respect to distribution $p \in \Delta(\mathcal{X} \times \mathcal{Y})$. If $p^* \in \Delta(\mathcal{X} \times \mathcal{Y})$ is the underlying distribution of the instance-label pairs, then $\ell(h, p^*)$ is the classification error probability or classification risk of rule $h$ denoted in the following as $\mathcal{R}(h)$, that is, $\mathcal{R}(h) := \ell(h, p^*)$.

Instance-label pairs can be represented as real vectors by using a feature mapping $\Phi : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}^m$. The most common way to define such feature mapping is using multiple features over instances together with one-hot encodings of labels as follows (see e.g., [Mohri et al., 2018])

$$\Phi(x, y) = e_y \otimes \Psi(x) = \left[ \mathbf{1}\{y = 1\} \Psi(x)^T, \ldots, \mathbf{1}\{y = |\mathcal{Y}|\} \Psi(x)^T \right]^T,$$

where the map $\Psi : \mathcal{X} \to \mathbb{R}^d$ represents instances as real vectors of size $d$. This map can be just the identity $\Psi(x) = x$ or given by a feature representation such as that provided by random Fourier features (RFF) [Rahimi and Recht, 2008], that is

$$\Psi(x) = \left[ \cos(u^T_1 x), \cos(u^T_2 x), \ldots, \cos(u^T_D x), \sin(u^T_1 x), \sin(u^T_2 x), \ldots, \sin(u^T_D x) \right]^T$$

for $D$ random Gaussian vectors $u_1, u_2, \ldots, u_D \sim N(0, \gamma I)$ with covariance given by the scaling parameter $\gamma$ (see e.g., Rahimi and Recht, 2008).

In this paper we consider scenarios in which the features’ dimensionality ($d$) is large, and propose efficient learning methods for the recently presented MRCs, which are briefly described in the following.

2.2 MINIMAX RISK CLASSIFIERS

MRCs are classification rules that minimize the worst-case error probability over distributions in an uncertainty set [Mazuelas et al., 2020, 2022, 2023]. Specifically, such rules are solutions to the minimax risk problem defined as

$$\min_{h \in T(\mathcal{X}, \mathcal{Y})} \max_{p \in \mathcal{U}} \ell(h, p)$$

where $\mathcal{U}$ is an uncertainty set of distributions determined by expectation estimates as

$$\mathcal{U} = \{p \in \Delta(\mathcal{X} \times \mathcal{Y}) : \mathbb{E}_p\{\Phi(x, y)\} - \tau \preceq \lambda\}$$

where $\tau$ denotes the mean vector of expectation estimates corresponding with the feature mapping $\Phi$, and $\lambda \succeq 0$ is a confidence vector that accounts for inaccuracies in the estimate. The mean and confidence vectors can be obtained from the training samples $\{(x_i, y_i)\}_{i=1}^n$ as

$$\tau = \frac{1}{n} \sum_{i=1}^n \Phi(x_i, y_i), \quad \lambda = \frac{8}{\sqrt{n}}$$

As described in Mazuelas et al., 2020, 2022, 2023 using the expected 0-1 loss $\ell$, the MRC rule $h$ solution of (3) is given by a linear combination of the feature mapping with coefficients given by a vector $\mu^* \in \mathbb{R}^m$. Specifically, the MRC rule $h$ given by $\mu^*$ assigns label $\hat{y} \in \mathcal{Y}$ to instance $x \in \mathcal{X}$ with probability

$$h(\hat{y}|x) = \begin{cases} (\Phi(x, \hat{y})^T \mu^* - \varphi(\mu^*))_+ / dx & \text{if } dx \neq 0 \\ 1/|\mathcal{Y}| & \text{if } dx = 0 \end{cases}$$

(6)
where \( \varphi(\mu) = \max_{x \in \mathcal{X}, C \subseteq \mathcal{Y}} \left( \sum_{y \in \mathcal{C}} \Phi(x, y)^T \mu - 1 \right) \)
\( \frac{1}{|C|} \)
\( d_x = \sum_{y \in \mathcal{Y}} (\Phi(x, y)^T \mu^* - \varphi(\mu^*))_+ \).

Note that the corresponding deterministic classification rule \( h_d \) assigns a label that maximizes the probability in (6) and is given by \( \arg \max_{y \in \mathcal{Y}} h(y|x) = \arg \max_{y \in \mathcal{Y}} \Phi(x, y)^T \mu^* \).

In addition, the classification risk of such classification rule \( h_d \) is bounded by twice the error probability of the MRC rule \( h \), that is,
\[
\mathcal{R}(h_d) \leq 2\mathcal{R}(h) \tag{7}
\]
since \( 1 - h_d(y|x) \leq 2(1 - h(y|x)) \) for any \( x \in \mathcal{X}, y \in \mathcal{Y} \).

The vector \( \mu^* \) that determines the 0-1 MRC rule corresponding to (5) is obtained by solving the convex optimization problem [Mazuelas et al., 2020, 2023]
\[
\mathcal{R}^* = \min_{\mu} \left( 1 - \tau^T \mu + \varphi(\mu) + \lambda^T |\mu| \right). \tag{8}
\]
The minimum value \( \mathcal{R}^* \) of (8) equals the minimax risk value of (3). Hence, it is the MRC’s worst-case error probability for distributions included in the uncertainty set \( \mathcal{U} \), and is an upper bound on the MRC’s classification error when the underlying distribution is included in such uncertainty set.

The convex optimization problem (8) of MRCs is L1-penalized and leads to sparsity in the coefficients \( \mu^* \) corresponding to the features in \( \Phi \). This sparsity in the coefficients implies that only a subset of features are sufficient to obtain the optimal worst-case error probability for MRCs. Therefore, in practice, efficient learning can be achieved by using the relevant subset of features in \( \Phi \) to solve the MRC optimization problem. This intuition leads to the efficient learning algorithm presented in this following.

## 3 EFFICIENT LEARNING OF MRCs IN HIGH DIMENSIONS

This section describes the proposed learning algorithm based on constraint generation over an LP formulation of MRCs learning (8).

### 3.1 LP FORMULATION FOR 0-1 MRCs

The theorem below presents an LP formulation (primal and dual) for the 0-1 MRC convex optimization problem (8).

**Theorem 1.** Let \( S \) be the set of pairs of instances and labels’ subsets, i.e., \( S = \{(x, C) : x \in \mathcal{X}, C \subseteq \mathcal{Y}, |C| \neq 0\} \), and for each \( i = 1, 2, \ldots, |S| \) corresponding to pair \((x, C)\) let
\[
g_i = \sum_{y \in \mathcal{C}} \Phi(x, y)^T \mu, \quad b_i = \frac{1}{|C|} - 1. \tag{9}
\]

Then, the 0-1 MRC problem (8) is equivalent to the LP
\[
\mathcal{P} : \min_{\mu_1, \mu_2, \nu} - (\tau - \lambda)^T \mu_1 + (\tau + \lambda)^T \mu_2 + \nu
\]
s.t.
\[
F(\mu_1 - \mu_2) - \nu 1 \leq b
\]
\[
\mu_1, \mu_2 \geq 0
\]
where the \( i \)-th row of matrix \( F \in \mathbb{R}^{S \times m} \) is given by \( g_i^T \), and the \( i \)-th component of vector \( b \in \mathbb{R}^{|S|} \) is given by \( b_i \).

In addition, the Lagrange dual of (10) is
\[
\mathcal{D} : \max \left\{ -b^T \alpha \right\}
\]
s.t.
\[
\tau - \lambda \preceq F^T \alpha \preceq \tau + \lambda
\]
\[
1^T \alpha = 1, \quad \alpha \succeq 0
\]
and if \( \mu^*_1, \mu^*_2, \nu^* \) is a solution of (10), we have that \( \mu^* = \mu^*_1 - \mu^*_2 \) is a solution of (8).

**Proof.** In the convex optimization problem (8), we introduce the additional variable \( \nu \in \mathbb{R} \) given by \( \nu = \varphi(\mu) + 1 \). Then, using \( g_i \) and \( b \) as defined above, we have
\[
\nu = \max_{i \in \{1, 2, \ldots, |S|\}} g_i^T \mu - b_i. \tag{12}
\]

Therefore, the optimization problem (8) becomes
\[
\min_{\mu, \nu} - \tau^T \mu + \lambda^T |\mu| + \nu
\]
s.t.
\[
F \mu - \nu 1 \leq b. \tag{13}
\]

The optimization in (13) can be reformulated as the LP in (10) using the change of variables \( \mu_1 = (\mu)_+ \) and \( \mu_2 = (-\mu)_+ \) which implies \( \mu = \mu_1 - \mu_2 \) and \( |\mu| = \mu_1 + \mu_2 \). Finally, the dual in (11) is directly obtained from the LP (10) (see e.g., Section 4.2 in [Bertsimas and Tsitsiklis 1997]).

The number of variables of the primal problem \( \mathcal{P} \) in (10) (constraints in dual problem \( \mathcal{D} \) in (11)) is given by the number of features of \( \Phi \), \( m = d|\mathcal{Y}| \). Therefore, the complexity of MRC learning given by such LP formulation is \( O(m^3) \) which is not affordable in high-dimensional settings. The next section presents an efficient learning algorithm for MRCs in high dimensions based on constraint generation methods.

### 3.2 ALGORITHM FOR EFFICIENT LEARNING

MRC learning can be efficiently carried out in high-dimensional settings because the solution of (10) is a sparse vector. This sparsity is due to the implicit L1-penalization in (8), \( \lambda^T |\mu| \), and the fact that usually only a small subset of features are informative in high-dimensional settings [Ghosh and Cabrera 2022]. The sparsity of the MRCs’ coefficients enables to carry out the learning process considering only a small subset of variables in (10) (respectively constraints in (11)). In the
following, we propose an algorithm based on constraint generation methods that solves the MRC LP problem in (10) by iteratively selecting small subsets of features of \( \Phi \).

**Algorithm 1** Efficient learning algorithm for 0-1 MRCs

**Input:** \( \mathbf{F}, \mathbf{b}, \tau, \lambda, \) initial subset of features \( \mathcal{I} \), dual constraints’ violation threshold \( \epsilon \), maximum number of iterations \( k_{\text{max}} \), and maximum number of features selected in each iteration \( n_{\text{max}} \)

**Output:** selected features \( \mathcal{I} \subseteq \{1, 2, \ldots, m \} \), optimal solution \( \mathbf{\mu}^* \in \mathbb{R}^m \), and optimal worst-case error probability \( R^* \)

1. \( \mathbf{\mu}^1 = [0, 0, \ldots, 0] \in \mathbb{R}^m \)
2. \( \text{LPSOLVE}(\mathcal{P}_\mathcal{F}) \)
   \( \mathbf{\mu}_1, \mathbf{\mu}_2, \nu^1 \leftarrow \text{Solution of primal} \)
   \( \alpha^1 \leftarrow \text{Solution of dual} \)
   \( R^1 \leftarrow \text{Optimal value (worst-case error probability)} \)
3. \( \mathbf{J} \leftarrow \text{SELECT}(\mathbf{F}, \tau, \lambda, n_{\text{max}}, \mathcal{I}, \epsilon, \alpha^1) \)
4. \( k = 1 \)
5. **while** \( \mathcal{J} \setminus \mathcal{I} \neq \emptyset \) and \( k \leq k_{\text{max}} \) **do**
   6. \( k = k + 1 \)
   7. \( \mathbf{\mu}_1^{k-1} = (\mathbf{\mu}_1^{k-1})_\mathcal{J}^+, \mathbf{\mu}_2^{k-1} = (\mathbf{\mu}_1^{k-1})_{\mathcal{J}}^- \)
   8. \( \text{LPSOLVE}(\mathcal{P}_{\mathcal{J}}, \mathbf{\mu}_1^{k-1}, \mathbf{\mu}_2^{k-1}, \nu^{k-1}) \)
   9. \( \mathbf{\mu}_1^k, \mathbf{\mu}_2^k, \nu^k \leftarrow \text{Solution of primal} \)
   10. \( \alpha^k \leftarrow \text{Solution of dual} \)
   11. \( R^k \leftarrow \text{Optimal value (worst-case error probability)} \)
   12. \( \mathbf{\mu}_2^k = \mathbf{\mu}_1^k - \mathbf{\mu}_2^k \)
   13. \( \mathcal{I} \leftarrow \mathcal{J} \)
   14. \( \mathcal{J} \leftarrow \text{SELECT}(\mathbf{F}, \tau, \lambda, n_{\text{max}}, \mathcal{I}, \epsilon, \alpha^k) \)
15. **end while**

The proposed learning algorithm obtains the optimal solution \( \mathbf{\mu}^* \) to the original problem by iteratively solving a sequence of subproblems (see details in Algorithm 1). These subproblems correspond with small subsets of features selected by a constraint generation method (SELECT function detailed in Algorithm 2).

The subproblem of (10) corresponding to the subset of features \( \mathcal{J} \subseteq \{1, 2, \ldots, m \} \) is defined as

\[
\mathcal{P}_{\mathcal{J}} : \min_{\mathbf{\mu}_1, \mathbf{\mu}_2, \nu} - (\mathbf{\tau}_\mathcal{J} - \mathbf{\lambda}_\mathcal{J})^T \mathbf{\mu}_1 + (\mathbf{\tau}_\mathcal{J} + \mathbf{\lambda}_\mathcal{J})^T \mathbf{\mu}_2 + \nu \\
\text{s.t.} \quad \mathbf{F}_\mathcal{J} (\mathbf{\mu}_1 - \mathbf{\mu}_2) + \nu \mathbf{1} \leq \mathbf{b} \\
\quad \mathbf{\mu}_1, \mathbf{\mu}_2 \succeq 0
\]

where \( \mathbf{\tau}_\mathcal{J} \) and \( \mathbf{\lambda}_\mathcal{J} \) denote the subvectors of \( \mathbf{\tau} \) and \( \mathbf{\lambda} \) correspondingly to the \( \mathcal{J} \) components, and \( \mathbf{F}_\mathcal{J} \) denotes the submatrix of \( \mathbf{F} \) corresponding to the \( \mathcal{J} \) columns. In addition, the dual of (14) is

\[
\mathcal{D}_{\mathcal{J}} : \max_{\alpha} - \mathbf{b}^T \alpha \\
\text{s.t.} \quad \mathbf{\tau}_\mathcal{J} - \mathbf{\lambda}_\mathcal{J} \leq \mathbf{F}_\mathcal{J}^T \alpha \leq \mathbf{\tau}_\mathcal{J} + \mathbf{\lambda}_\mathcal{J} \\
\quad 1^T \alpha = 1, \alpha \succeq 0.
\]

At each iteration \( k \) of Algorithm 1 (Line 9), the LPSOLVE function solves such subproblems and obtains the primal solution \( \mathbf{\mu}_1^k, \mathbf{\mu}_2^k, \nu^k \) and dual solution \( \alpha^k \) along with the worst-case error probability \( R^k \) given by the optimal value. The dual solution is used by the SELECT function (Line 4 and 13) to obtain a subsequent subset of features. The primal solution can be used by the LPSOLVE function (Line 9) to warm-start the optimization in the next iteration. This iterative process ends when the SELECT function returns a subset of features that does not contain any new feature.

Notice that at each iteration \( k \), the algorithm obtains coefficients \( \mathbf{\mu}_k \), features subset \( \mathcal{J} \), and worst-case error probability \( R^k \). In Section 3.3 we show that such coefficients \( \mathbf{\mu}_k \) provide an MRC with worst-case error probability \( R^k \) corresponding with the uncertainty set given by features \( \mathcal{J} \). In addition, we show that such worst-case error probability monotonically decreases with the number of iterations and converges to the optimal corresponding with all the features.

### 3.3 Greedy Feature Selection

The SELECT function determines the subset of features for the next iteration based on the previous subset and the current solution. Specifically, this greedy selection process selects features corresponding to the most violated constraints in the dual and removes features corresponding to the constraints satisfied with a positive slack (oversatisfied constraints). Such a process aims to achieve the fastest decrease in worst-case error probability while using the smallest number of features. As described in the literature for constraint generation methods [Bertsimas and Tsitsiklis 1997][Desrosiers and Lübbecke 2005], this type of selection process can be implemented in several alternative ways such as adding any subset of violated constraints or not removing constraints. In practice, we observe that adding a subset of violated constraints and removing all the oversatisfied constraints achieves the fastest convergence.

The implementation details for function SELECT are provided in Algorithm 2. The vector \( \nu \) quantifies the violations in the dual constraints. In particular, the features corresponding to the negative values of vector \( \nu \) (oversatisfied constraints) are removed, and the features corresponding to the \( n_{\text{max}} \) largest positive values of vector \( \nu \) are added. Moreover, the selection of features is also restricted by hyperparameter \( \epsilon \geq 0 \) that represents the minimum vio-
Algorithm 2 SELECT (greedy feature selection)

**Input:** \( F, \tau, \lambda, n_{\text{max}}, \) current subset of features \( I, \) dual constraints’ violation threshold \( \epsilon, \) and dual solution \( \alpha \)

**Output:** selected features \( J \subseteq \{1, \ldots, m\} \)

1. \( v = \|F^T \alpha - \tau\| - \lambda \)
2. \( J = \{i : i \in I, v_i = 0\} \)
3. \( A \leftarrow \text{ARGMAX}(v, n_{\text{max}}) \)
4. \( A = \{i : i \in A, v_i > \epsilon\} \)
5. \( J \leftarrow J \cup A \)

The following shows the theoretical properties of the proposed learning algorithm. In particular, the algorithm’s iterations provide a sequence of MRCs with decreasing worst-case error probabilities that converges to the MRC corresponding with all the features.

3.4 COMPUTATIONAL COMPLEXITY

The computational complexity of Algorithm 2 is given by the number of iterations and the complexity per iteration that depend on the maximum number of features selected in each iteration \( n_{\text{max}} \) and the hyperparameter \( \epsilon. \) Decreasing \( n_{\text{max}} \) results in a reduced complexity per iteration at the expense of an increased number of iterations. Increasing \( \epsilon \) can decrease the number of iterations and complexity per iteration at the expense of achieving approximate solutions. For instance, if \( n_{\text{max}} = m \) and \( \epsilon = 0 \) the algorithm finds the exact solution in only one iteration but the complexity of such iteration is large. In Section 4, we show that in practice \( \epsilon = 0.0001 \) and \( n_{\text{max}} \in [50, 500] \) obtains efficient and accurate learning of MRCs.

The number of iterations can be further reduced by using an adequate choice for the initial subset of features. This initial subset of features \( I \) can be obtained efficiently using a simple approach for coarse feature selection such as correlation screening or few iterations of a first order optimization method. Similarly, the complexity per iteration is reduced by using a warm-start in LPSOLVE. In the proposed algorithm, a warm-start for iteration \( k \) is obtained directly from the previous solution \( \mu^{k-1} \) of the LP at iteration \( k-1 \). Note that this warm-start is a basic feasible solution for the LP at iteration \( k \) since it is obtained by removing and adding features for which the corresponding coefficients at \( k-1 \) are zero.

3.5 THEORETICAL ANALYSIS OF THE ALGORITHM

The following shows the theoretical properties of the proposed learning algorithm. In particular, the algorithm’s iterations provide a sequence of MRCs with decreasing worst-case error probabilities that converges to the MRC corresponding with all the features.

Theorem 2. Let \( \mu^k \) and \( R^k \) be the coefficients and worst-case error probability obtained by the proposed algorithm at iteration \( k. \) If \( h^k \) is the MRC given by \( \mu^k, \) then we have

\[
R(h^k) \leq R^k + \left( |E_{\Phi^k} \cdot (\Phi(x, y)_J) - \tau_J| - \lambda_J \right)^T |\mu^k_J| \tag{16}
\]

where \( J \) is the subset of features used at iteration \( k. \) In addition, the algorithm provides MRCs with decreasing worst-case error probabilities, that is,

\[
R^{k+1} \leq R^k, \; k = 1, 2, \ldots \tag{17}
\]

Proof. At each intermediate step, \( \mu^k \) and \( R^k \) are the coefficients and worst-case error probability of the MRC corresponding with uncertainty set

\[
U^k = \{ p \in \Delta(X \times \mathcal{Y}) : |E_{\Phi^k} \cdot (\Phi(x, y)_J) - \tau_J| \leq \lambda_J \} \tag{18}
\]

using Theorem 1 for the subproblem. Therefore, inequality \( 16 \) is obtained using the bounds for error probabilities for MRCs. The second result is obtained since the warm-start at iteration \( k+1 \) is a feasible solution with an objective value that equals the worst-case error probability \( R^k \) at iteration \( k. \) The warm-start is feasible at \( k+1 \) and has value \( R^k \) because it is obtained from the solution at iteration \( k \) by removing and adding features corresponding to zero coefficients.

Inequality \( 16 \) bounds the classification error of the MRC classifier at any intermediate iteration. Specifically, the worst-case error probability \( R^k \) at any iteration \( k \) corresponding to a feature subset \( J \) directly provides such a bound if the error in the mean vector estimate is not underestimated, i.e., \( \lambda_J \geq |E_{\Phi^k} \cdot (\Phi(x, y)_J) - \tau_J|. \) In particular, if \( \lambda_J \) is a confidence vector with coverage probability \( 1-\delta, \) that is, \( \mathbb{P}\{ |E_{\Phi^k} \cdot (\Phi(x, y)_J) - \tau_J| \leq \lambda_J \} \geq 1-\delta, \) then

\[
R(h^k) \leq R^k \tag{19}
\]

with probability at least \( 1-\delta. \) In other cases, \( R^k \) still provides approximate bounds as long as the underestimation \( |E_{\Phi^k} \cdot (\Phi(x, y)_J) - \tau_J| - \lambda_J \) is not substantial. Similar bounds also hold for the sequence of deterministic classification rules due to inequality \( 16. \)

The next theorem shows the convergence of the sequence of MRCs obtained by the proposed algorithm to the MRC corresponding with all the features.

Theorem 3. Let \( \mu^* \) and \( R^* \) be the MRC coefficients and worst-case error probability obtained by solving \( 10 \) using
all the features. If $R^k$, $k = 1, 2, \ldots$, is the sequence of worst-case error probabilities obtained by the proposed algorithm using dual constraints’ violation threshold $\epsilon$. Then, there exists $k_0 \geq 1$ such that

$$R^* \leq R^k \leq R^* + \epsilon\|\mu^*\|_1$$

(20)

for any $k \geq k_0$.

Proof. The first inequality follows by noting that the feasible set of (11) corresponding with all the features is contained in the feasible set of any subproblem given a subset of features. In the following, we prove the second inequality.

Let $k_0 \geq 1$ be an iteration in which SELECT function in Algorithm 1 does not add any new feature. Such a case occurs after a finite number of iterations due to the properties of constraint generation methods [Bertsimas and Tsitsiklis 1997]. If $\alpha_{k_0}$ is the dual solution obtained at iteration $k_0$ with subset of features $\mathcal{F}$, then we have that

$$\tau_{\mathcal{F}} - \lambda_{\mathcal{F}} \leq F_{\mathcal{F}} \alpha_{k_0} \leq \tau_{\mathcal{F}} + \lambda_{\mathcal{F}}$$

(21)

$$\tau_{\mathcal{F}} - \lambda_{\mathcal{F}} - \epsilon 1 \leq F_{\mathcal{F}} \alpha_{k_0} \leq \tau_{\mathcal{F}} + \lambda_{\mathcal{F}} + \epsilon 1.$$  

(22)

On combining (21) and (22), we have

$$\tau - \lambda - \epsilon 1 \leq F \alpha_{k_0} \leq \tau + \lambda + \epsilon 1.$$  

(23)

Now, consider the following primal problem corresponding to the dual (11) with constraints as in (23).

$$\min_{\mu_1, \mu_2, \nu} - (\tau - \lambda - \epsilon 1)^T \mu_1 + (\tau + \lambda + \epsilon 1)^T \mu_2 + \nu$$

s.t.

$$F^T(\mu_1 - \mu_2) - \nu 1 \leq c$$

$$\mu_1, \mu_2, \nu \geq 0.$$  

(24)

If $\mu_1^*, \mu_2^*$, and $\nu^*$ correspond to the MRC coefficients obtained by solving (10) using all the features, then it is also a feasible solution to the problem (24) since they have the same feasible set. Therefore, using weak duality (Theorem 4.3 in Bertsimas and Tsitsiklis 1997)), we have that

$${\bf b}^T \alpha_{k_0} \leq -(\tau - \lambda - \epsilon 1)^T \mu_1^* + (\tau + \lambda + \epsilon 1)^T \mu_2^* + \nu^*$$

(25)

since $\alpha_{k_0}$ is a feasible solution for the dual of (24). Therefore,

$$R^{k_0} \leq R^* + \epsilon 1 (\mu_1^* + \mu_2^*) = R^* + \epsilon \|\mu^*\|_1$$

(26)

since $\mu_1^* = (\mu^*)_+$ and $\mu_2^* = (-\mu^*)_+$. Hence, the second inequality holds for any $k \geq k_0$ since $R^k \leq R^{k_0}$ due to the monotonic decrease of the worst-case error probability shown in Theorem 2.

4 RESULTS

In this section, we present a set of experimental results that analyze the effect of hyperparameters and quantify the training time improvements in practice. In addition, we describe the benefits of having the worst-case error probabilities and show that the presented algorithm performs efficient feature selection. The proposed Algorithm 1 (MRC-CG) is compared with the LP formulation for MRCs in [10] using all the features (MRC-LP), and the constraint generation method for L1-SVMs (SVM-CG) [Dedieu et al. 2022]. In addition, the quality of the feature selection is compared with SVM-CG, recursive feature elimination (RFE) for SVMs [Guyon et al., 2002], minimum redundancy maximum relevancy (MRMR), and analysis of variance (ANOVA) [Ding and Peng, 2005; Peng et al., 2005]. The experimental results are obtained using 13 real-world high-dimensional datasets as shown in Table 1. The datasets 4 and 10 can be obtained from the UCI [Dua and Graff, 2017] repository and the remaining from https://jundongl.github.io/scikit-feature/datasets.html. The implementation of the algorithm proposed is available in the library MRCpy [Bondugula et al. 2023] and the experimental setup is https://github.com/MachineLearningBCAM/Constraint-Generation-for-MRCs.

The hyperparameter $\epsilon$: We present results that show the influence of $\epsilon$, and illustrate in practice the theoretical prop-
The worst-case error probability $R^*$ is obtained by solving (10) using all the features and the sequence of worst-case error probabilities $R^k$ is obtained by MRC-CG for increasing number of iterations $k$. In Figure 1, we show the convergence of $R^k$ to $R^*$ using $\epsilon = \{0.01, 0.001, 0.0001\}$ and $n_{max} = 100$. In practice, we observe that $R^k$ converges to $R^*$ with differences at most in the order of $10^{-3}$ even for $\epsilon = 0.01$. In addition, the results show that $R^k$ is monotonically decreasing (as shown in Theorem 2) and achieves significant convergence in few iterations. We also observe that the smaller values of $\epsilon$ lead to more accurate results, as shown in Theorem 3. On average, highly accurate results are obtained in 20 iterations using $\epsilon = 0.0001$.

The hyperparameter $n_{max}$: We present results that show the influence of the hyperparameter $n_{max}$ on the training time of MRC-CG in comparison with MRC-LP using datasets "Prostate_GE", "Arcene", "Ovarian" and "SMK_CAN_187". The parameters of MRC-CG are taken as $\epsilon = 0.0001$ and $k_{max} = 20$, and the training times are averaged over 50 random repetitions using 90% of the data. Figure 2 presents the relative time computed as the time taken by MRC-CG over the time taken by MRC-LP for values of $n_{max}$ in the range of 1 to 1,500. The figure shows the trade-off due to the choice of hyperparameter $n_{max}$. Increasing the value of $n_{max}$ decreases the number of iterations for convergence at the expense of increasing the complexity per iteration. In practice, with $n_{max}$ in the interval [50, 500], we obtain a good compromise between the number of iterations required for convergence and the complexity per iteration. On average, for $n_{max} = 100$, MRC-CG is 10 times faster than MRC-LP. Based on these results, in the remainder of this section we take $n_{max} = 100$, $\epsilon = 0.0001$, and $k_{max} = 10$.

Scalability with increasing number of features: We present results to compare the scalability of MRC-CG with MRC-LP, and SVM-CG for increasing number of features on the datasets "Ovarian" and "Arcene". In particular, the results show the effect of the number of features on the training time of MRC-CG and compare it with MRC-LP and SVM-CG. The number of features range from 100 to 25,000 obtained using RFFs. Figure 2 presents the average training times for MRC-CG, MRC-LP, and SVM-CG over 20 random repetitions. We observe that MRC-CG is faster than MRC-LP for all cases and improves the scaling with the number of features significantly better than MRC-LP. In addition, the training times of MRC-CG are competitive with training times of SVM-CG, especially for large number of features.
Comparison using real-world datasets: Table 2 presents results to compare the average training times for MRC-CG and SVM-CG using the 13 high-dimensional datasets. We observe that MRC-CG is competitive with the SVM-CG in terms of training times. In addition, Table 2 presents worst-case error probability $R^*$ given by MRC-CG along with the 10-fold cross-validated error estimate. We observe that the worst-case error probability $R^*$ obtained using all the data at training can provide an error assessment for MRC-CG without requiring cross-validation. For instance, the $R^*$ is in the confidence interval of the estimated error in 8 out of 13 datasets, and is an upper bound to the confidence interval of the estimated error in the remaining datasets. This worst-case error probability is particularly useful in the addressed setting since the scarcity of training samples results in a high variability for the error estimates based on cross-validation, as shown in the table.

Feature selection: Table 3 presents results to compare the MRC-CG as a feature selection approach with SVM-CG, RFE, MRMR, and ANOVA. The table shows the 10-fold cross-validated errors for logistic regression (LR) and decision tree (DT) using the features selected by the different methods. We assess the quality of features selected based on the errors and the number of features selected. Note that the number of features selected by RFE, MRMR, and ANOVA were set to the number of features selected by SVM-CG. The errors show that the presented MRC-CG provides state-of-the-art results for feature selection and can effectively select the most relevant features.

5 CONCLUSION

In this paper, we presented a learning algorithm for the recently proposed minimax risk classifiers (MRCs) that is efficient in high-dimensional settings. The algorithm utilizes
Table 3. Comparison of number of features selected and the error estimate obtained for logistic regression (LR) and decision tree (DT) using MRC-CG in comparison with multiple methods for feature selection.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>MRC-CG</th>
<th>SVM-CG</th>
<th>RFE</th>
<th>MRMR</th>
<th>ANOVA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Error</td>
<td>No. of features</td>
<td>Error</td>
<td>No. of features</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>LR</td>
<td>DT</td>
<td>LR</td>
<td>DT</td>
<td>LR</td>
</tr>
<tr>
<td>1</td>
<td>.29 ± .10</td>
<td>.33 ± .06</td>
<td>172 ± 3</td>
<td>.27 ± .11</td>
<td>.41 ± .09</td>
</tr>
<tr>
<td>2</td>
<td>.20 ± .10</td>
<td>.19 ± .10</td>
<td>33 ± 2</td>
<td>.19 ± .10</td>
<td>.22 ± .13</td>
</tr>
<tr>
<td>5</td>
<td>.23 ± .13</td>
<td>.17 ± .12</td>
<td>76 ± 0</td>
<td>.14 ± .07</td>
<td>.29 ± .11</td>
</tr>
<tr>
<td>7</td>
<td>.04 ± .06</td>
<td>.12 ± .09</td>
<td>63 ± 1</td>
<td>.02 ± .05</td>
<td>.15 ± .12</td>
</tr>
<tr>
<td>10</td>
<td>.00 ± .00</td>
<td>.02 ± .02</td>
<td>118 ± 6</td>
<td>.00 ± .00</td>
<td>.01 ± .02</td>
</tr>
<tr>
<td>11</td>
<td>.08 ± .06</td>
<td>.16 ± .08</td>
<td>77 ± 2</td>
<td>.10 ± .08</td>
<td>.13 ± .10</td>
</tr>
<tr>
<td>12</td>
<td>.29 ± .12</td>
<td>.41 ± .11</td>
<td>135 ± 3</td>
<td>.27 ± .09</td>
<td>.37 ± .09</td>
</tr>
</tbody>
</table>

A greedy feature selection approach that iteratively removes and selects features achieving a fast decrease in worst-case error probability while using a small number of features. We prove theoretically that the proposed iterative algorithm obtains a sequence of MRCs with decreasing worst-case error probabilities that converge to the solution obtained using all the features. The numerical results assess the efficiency of the presented algorithm and compare it with the state-of-the-art using 13 high-dimensional datasets with a large number of features. The results show that the presented algorithm converges to the solution obtained using all the features in a few iterations, and provides a significant efficiency increase, especially in cases with a large number of features. In addition, the algorithm provides the worst-case probability error that is particularly useful in high-dimensional scenarios with limited number of samples, which can suffer from a high variability of assessments based on cross-validation. The results also show that the algorithm can provide state-of-the-art results for feature selection and can effectively select the most relevant features.

Acknowledgements

Funding in direct support of this work has been provided by projects PID2019-105058GA-100, CNS2022-135203, and CEX2021-001142-S funded by MCIN/AEI/10.13039/501100011033 and the European Union “NextGenerationEU”/PRTR, and by programmes ELKARTEK and BERC-2022-2025 funded by the Basque Government.

References


