Supervised Classification and Mathematical Optimization *

EMILIO CARRIZOSA
Universidad de Sevilla (Spain)
ecarrizosa@us.es

DOLORES ROMERO MORALES
University of Oxford (United Kingdom)
dolores.romero-morales@sbs.ox.ac.uk

June 20, 2012

Abstract

Data Mining techniques often ask for the resolution of optimization problems. Supervised Classification, and, in particular, Support Vector Machines, can be seen as a paradigmatic instance. In this paper, some links between Mathematical Optimization methods and Supervised Classification are emphasized. It is shown that many different areas of Mathematical Optimization play a central role in off-the-shelf Supervised Classification methods. Moreover, Mathematical Optimization turns out to be extremely useful to address important issues in Classification, such as identifying relevant variables, improving the interpretability of classifiers or dealing with vagueness/noise in the data.

Keywords: Data Mining, Mathematical Optimization, Support Vector Machines, Interpretability, Cost Efficiency.

*This work has been partially supported by projects MTM2009-14039 and FQM-329 of Junta de Andalucía, Spain.


1 Introduction

One of the most important tasks in Data Mining, [116, 121, 240], is *Supervised Classification*, which seeks procedures for classifying objects in a set $\Omega$ into a set $C$ of classes. Each object $u \in \Omega$ has associated a pair $(x^u, y^u)$, where $x^u$, the *predictor vector*, takes values on a set $X$, usually assumed to be a subset of $\mathbb{R}^p$, and $y^u \in C$ is the class membership of $u$. Hereafter, we will simply use the term *variable* to refer to each component of the predictor vector.

Not all the information about the objects in $\Omega$ is available: the class membership $c^u$ is only known for those objects $u$ in some subset $I \subset \Omega$, called the *training sample*.

With this information, a classification rule is sought, i.e., a function $y : X \to C$, which assigns label $y(x) \in C$ to predictor vector $x$, $\forall x$.

In its basic form, $C$ consists of a finite set of nominal values, without an intrinsic ranking (e.g. $C = \{\text{benign, malign}\}$), though part of the theory extends to the case in which $C$ is a finite set equipped with an order relation, or a segment of the real line. In this latter case, we would have a regression problem instead, [216].

Supervised Classification has been successfully applied in many different fields. Examples are found in Text Categorization [210], such as document indexing, webpage classification and spam filtering; Biology and Medicine, such as classification of gene expression data [102, 245], homology detection [143], protein-protein interaction prediction [28, 171], abnormal brain activity classification [55] and cancer diagnosis [110, 165]; Machine Vision [75, 188]; Agriculture [179]; or Chemistry [60], to cite a few fields and references.

We can argue that business applications have had a later start. Despite of this, nowadays we can find many applications of Supervised Classification in Marketing, Customer Relationship Management, Banking, among others, [4, 5, 115, 144, 153, 175]. Typical business applications are credit scoring [11], bankruptcy [176], fraud detection [87], customer targeting [73], customer loyalty [106, 112], market basket analysis [61], recommender systems [62], revenue management [122], services booking cancellations [203], country risk ratings [114], prediction of health costs [24] or stock market forecast [103, 156].

Mathematical Optimization has played a crucial role in Supervised Classification [21, 22, 31, 32, 84, 81, 88, 107, 218, 242]. Techniques from very diverse fields within Mathematical
Optimization have been shown to be useful. As we will discuss in Section 3, and already pointed out e.g. in [17], many of the optimization problems encountered fall within the area of (smooth) Convex Programming. However, other areas of Mathematical Optimization play a notable role, among others, Global Optimization [9, 13, 51, 128, 160, 245], Linear Programming [94, 158, 205] Mixed-Integer Programming [25, 39, 50, 77, 220, 228], Nonsmooth Optimization [7, 13, 44, 51, 222, 223], Multicriteria and Multi-Objective Programming [68, 93, 181, 248] and Robust Optimization [224].

The success of Mathematical Optimization when applied to Supervised Classification has one of its main exponents in Support Vector Machines (SVM) [30, 72, 229, 230], a technique rooted in Statistical Learning Theory [229, 230], which has proved to be one of the state-of-the-art methods for Supervised Learning. For the 2-class case, SVM aims at separating both classes by means of a hyperplane which maximizes the margin, i.e., the width of the band separating the two sets. This geometrical optimization problem can be written as a convex quadratic optimization problem with linear constraints, in principle solvable by any nonlinear optimization procedure. See also [18, 40, 108, 177, 113] for introductory surveys on SVMs.

The purpose of this paper is to illustrate that Mathematical Optimization is at the core of Supervised Classification methods. Moreover, the variety of algorithmic tools which have been used is rather wide, implying that the researchers in different branches of Mathematical Optimization have ample room to translate their expertise into this context, and they may find new domains of applicability to existing Mathematical Optimization knowledge. We stress that the aim of this paper is not to study in depth Classification methods, and we refer the reader to [36, 121, 125, 197, 201] for further details. Instead, our aim is to illustrate the central role played by Mathematical Optimization in such methods.

Due to its performance and its optimization context, we have a special focus on SVMs. The two basic versions of SVM, namely, the hard and soft margin approaches, are introduced. We then move on to the embedding of the variable space into a feature space of higher dimension, and the kernel version of SVM. We discuss the optimization problem behind the SVM, as well as the Mathematical Optimization techniques that have been proposed to solve it. We devote the rest of the paper to extensions of SVM dealing with critical issues such as interpretability,
cost efficiency or robustness, as well as dealing with data that may be unbalanced, imprecise or unlabeled. We will show that many different domains in Mathematical Optimization are needed to cope with both the standard SVM formulation as well as the variants addressing the properties mentioned above.

The remainder of the paper is organized as follows. In Section 2 we briefly discuss off-the-shelf classification methods and the role of Mathematical Optimization. In Section 3 we introduce the SVM, including the hard and soft versions as well as its kernelization. In Section 4 we discuss the Mathematical Optimization techniques proposed in the literature to build SVMs. In Section 5 we discuss critical modeling issues and how Mathematical Optimization can help to incorporate them into the original SVM model. Finally, conclusions are provided in Section 6.

2 Classification methods

Different classification methods have been proposed in the literature. They mainly differ in the statistical assumptions made of the data and the type of algorithms needed to construct the classifier. In this section we review benchmarking classification methods divided into three main categories: linear classifiers, nearest-neighbor classifiers and classification trees. The methods proposed have a deep geometrical flavor. For data sets in very low dimension, Computational Geometry tools may be useful, [23]. However, most real world data sets of interest are in larger dimension, calling for numerical rather than geometrical procedures.

Before presenting the benchmarking classification methods, we briefly discuss two important ingredients in Supervised Learning: the scoring functions, a general framework used to describe the classifier, and the performance criteria used to compare classification methods.

2.1 Scoring functions

The methods reviewed below are based on scoring functions: for each $c \in C$, a scoring function $f_c : X \rightarrow \mathbb{R}$ is built from the training set $I$, and forthcoming objects with predictor vector $x$ are classified as members of the class $y(x)$ with highest score. In other words, the classifier is
given by the function
\[ y(x) \in \arg\max_{c \in C} f_c(x). \] (1)

In case of ties, objects are randomly assigned to one of the classes at which the maximum is attained.

The scoring function \( f_c \) ranks the objects, so that, the higher the value of \( f_c(x) \), the higher the likelihood that an object represented by \( x \) is in class \( c \).

Obviously, the very same classifier is obtained if each \( f_c \) is replaced by \( f_c + h \) for a common \( h \), across all classes. Hence, we may set one of the scoring functions equal to zero. In the 2-class case, namely \( C = \{-1, 1\} \), setting \( f_{-1} = 0 \), (1) takes the form

\[ y(x) = \text{sign}(f_1(x)) \] (2)

where \( \text{sign}(a) = 1 \) if \( a > 0 \), and \(-1\) is \( a < 0 \).

### 2.2 Performance criteria

Comparing classification methods and then choosing a best-possible one is not an easy task, since several criteria are to be considered.

The main criterion is the so-called generalization power, i.e., how good the constructed classifier would correctly classify forthcoming objects, assumed to be generated from the same unknown random distribution than the training sample \( I \). In other words, one fundamental criterion is the minimization of the probability of misclassifying an object distributed as those in \( I \). Since such distribution is not known, the probability of misclassification is replaced by a surrogate, usually in the form of an estimate of the misclassification rate on \( I \). The most well-known instance is the so-called the \( k \)-fold crossvalidation error estimate, [136]. In \( k \)-fold crossvalidation, the original training set \( I \) is split into \( k \) subsets, \( I_1, \ldots, I_k \), of similar size. Each subset \( I_j \) is used to test how the classifier constructed from \( I \setminus I_j \) behaves. Hence, for each \( j = 1, 2, \ldots, k \), a classifier is constructed from the data in \( I \setminus I_j \) and tested on \( I_j \), yielding an accuracy \( a_j \). Such accuracy may be, for instance, the fraction of correctly classified individuals in \( I_j \). Averaging the \( k \) estimates \( a_j \) one obtains the \( k \)-fold crossvalidation estimate \( \frac{1}{k} \sum_{j=1}^{k} a_j \).
Different criteria are needed when the misclassification costs differ among the classes. The most popular performance measure here is the so-called area under the Receiver Operating Characteristic (ROC) curve, AUC. As it will become apparent below, the larger the AUC the better the classifier. In order to generate the ROC curve for a 2-class problem, the classifier (2) is replaced by the parametric class of classifiers

\[ y(x) = \text{sign}(f_1(x) - \vartheta), \tag{3} \]

where \( \vartheta \) reflects our willingness for classifying in class 1. The ROC curve shows the sensitivity, i.e., the proportion of correctly classified objects of class 1, against the specificity, i.e., the proportion of correctly classified objects of class \(-1\), for different values of the parameter \( \vartheta \).

For a fully random classification, the ROC curve is given by the segment joining the points \((0,0)\) and \((1,1)\), and thus, classification methods better than fully random classification lead to ROC curves above such segment, with a larger area under their ROC curve. See e.g. [69] for further details.

Other criteria are of great interest when comparing classification methodologies. These include, among others, their capability to successfully handle large-dimensional data sets or different data structures (e.g. categorical, graphical or functional data), or the comprehensibility of the classifier obtained, usually measured in terms of the complexity of the classifier, e.g., the number of parameters involved.

Other, algorithmically oriented, criteria have been proposed in [22]. These refer to the algorithms available to address the classification problem, and they include their scalability to handle large data sets, their performance in terms of running times and memory requirements, easiness to implement, and robustness and numerical stability.

Choosing a classifier taking into account these different performance measures yields multicriteria problems, for which multicriteria methodologies have been advocated, [141].

Having said this, we remark that no method systematically outperforms the remaining ones, even if only generalization is considered as relevant criterion.
2.3 Linear classifiers

Simple classifiers are obtained if one assumes the scoring functions $f_c$ in (1) to be affine, $f_c(x) = \omega_c^\top x + \beta_c$, and thus the locus of $x$ labeled as elements of class $c$, i.e., $y(x) = c$, is the polyhedron $X_c$:

$$X_c = \{ x \in \mathbb{R}^p : \omega_c^\top x + \beta_c \geq \omega_c'^\top x + \beta_c' \quad \forall c' \in C \}. \tag{4}$$

The literature on linear classifiers is vast, and the role of Mathematical Optimization is very important.

The first attempt is due to Fisher, [92]: it is sought the linear combination of the variables such that the so-called between-class variance is maximized relative to the so-called within-class variance. This reduces to a generalized eigenvalue problem, see e.g. Chapter 4 of [121].

A closely connected classifier is obtained in Linear Discriminant Analysis, LDA for short, which is summarized as follows. For each class $c$, the predictor vector $x$ of individuals in group $c$ is assumed to follow a gaussian distribution with mean vector $\mu_c$ and common covariance matrix $\Sigma$. Moreover, the prior probability $\pi_c$ of an incoming individual of being in group $c$ is also given. For a given predictor vector $x$, the posterior probability $p_c(x)$ of each class is calculated by the Bayes theorem, and then classification is done following the Bayes rule: an object is classified in its most (posterior) probable class. This corresponds to (1), with the scoring function $f_c$ given by

$$f_c(x) = x^\top \Sigma^{-1} \mu_c - \frac{1}{2} \mu_c^\top \Sigma^{-1} \mu_c + \log(\pi_c). \tag{5}$$

In practice, the parameters $\pi_c$, $\mu_c$ and $\Sigma$ are not known but they can be estimated via sample estimates.

Other popular linear classifiers are the classical logistic regression (LR), [121], and the linear programming models proposed by Mangasarian in [158, 159]. In LR, the log of the odds is modeled with an affine function of the predictor vector, $\log \left( \frac{p_1(x)}{p_{-1}(x)} \right) = \beta_0 + \beta^\top x$, where the parameters $\beta_0$ and $\beta$ are estimated using maximum likelihood estimates, which amounts to solving a nonlinear optimization problem. In [158], a linear programming model is derived to decide whether two sets are linearly separable, while in [159] the goal is to minimize the empirical error, i.e., the number of misclassified objects, yielding a linear programming model.
with equilibrium constraints.

The success of Mathematical Optimization when applied to Supervised Classification has one of its main exponents in Support Vector Machines (SVM) [30, 72, 229, 230]. Sections 3-5 are devoted to SVM and how critical modeling issues can be incorporated into SVM with the help of Mathematical Optimization.

Finally, just to remark that linear classifiers have also been sought from a different perspective. For instance, in the Artificial Intelligence literature, we find the so-called Perceptron algorithm of Rosenblatt, [204], seeking a linear classifier for linearly separable sets. With the aim of correctly classifying all elements in the training set $I$, a feasible solution of a system of linear inequalities is found by means of a heuristic procedure. See [72] for more details.

### 2.4 Nearest-Neighbors methods

Linear classifiers, as those introduced in Section 2.3, require the data to be in a vector space. Whereas one can overcome this limitation, for instance, using so-called kernels, see Section 3.4, a natural framework consists of defining a classifier via a dissimilarity measure $\delta$ in $X$, [129]. Roughly speaking, we may define $\delta$ as a metric on $X$, though triangle inequality and even positive-definiteness may not be required, and the classification rule is based on the fact that objects similar to each other should share the same label.

In the basic $k$-nearest neighbors method, [71, 74], for a given $x \in X$, let $N_k(x)$ the set of $k$ objects in the training sample $I$ closest to $x$, where closeness is measured via the dissimilarity $\delta$. Then, $x$ will be labeled with the most frequent class $c$ in $N_k(x)$. In other words, the $k$-nearest neighbors rule has the form (1), where $f_c(x)$ is equal to the cardinality of the subset of $N_k(x)$ with label $c$. See [78] for an analysis from the Statistical Learning perspective.

Mathematical Optimization appears in three different ways in $k$-nearest neighbors methods, namely evaluation of $\delta$, choice of $\delta$, and data (prototype) selection.

With respect to the evaluation of $\delta$, observe that, although $\delta$ is usually given via a closed formula, e.g., the Euclidean distance between objects in the $p$-dimensional Euclidean space, this is not always the case. In a variety of fields, such as Computational Biology, Text Processing or Speech Recognition, objects are represented as strings of symbols in a finite alphabet. A
A popular dissimilarity measure is the so-called edit distance, which, given two objects, counts
the minimum number of symbols deletions, insertions and substitutions needed to transform
one object into the other. Computing the edit distance between two objects can be done in
polynomial time using Dynamic Programming, [232]. More complex structures, such as trees,
or, even more generally, graphs, appear naturally in many real world data sets of biological
sequences, or semi-structured texts such as HTML or XML, [206, 126, 246]. Computing in these
cases a dissimilarity δ for a given pair of objects may lead to hard combinatorial optimization
problems, [27].

The performance of k-nearest neighbors methods clearly depends on the choice of δ. In some
instances, objects are already represented as points in a finite-dimensional Euclidean space.
However, instead of directly using as δ the Euclidean distance, or any fixed transform, as in
[119], we may consider a parameterized class Δ of distances and choose the one optimizing a
given performance measure. The simplest choice is to take as Δ the class of weighted Euclidean
distances and choose δ ∈ Δ, or equivalently, the weights, by solving an optimization problem.
This is suggested, among others, in [190], where, for each object i in the training set I, a
distance function δω,i : IR^p → IR is defined to measure distances from points z ∈ IR^p to
x^i as δω,i(z) = \sqrt{\sum_{j=1}^{p} (ω_j)^2 (z_j - x_{ij})^2}, and the nearest-neighbors method is used with the
so-obtained set of distances. The parameters ω^i ∈ IR^p are sought so that the so-called leave-
one-out (|I|-fold crossvalidation) misclassification estimate is minimized. A smoothed version of
the objective function (otherwise, piecewise constant) is locally optimized using a gradient-type
method. See also [189].

Prototype selection [154, 189] is another source of Mathematical Optimization problems in
k-nearest neighbors methods. Classifying a forthcoming individual x amounts to calculating
δ(x, z) for all records z in the data set. This operation may be very time consuming when
the number of records is large or when computing δ is a heavy task, as happens, for instance,
when computing δ amounts to solving a nontrivial optimization problem, as mentioned above.
How to conveniently select a subset of representative records, the so-called prototypes, leads
to large-scale combinatorial optimization problems, in general, hard to solve. For instance,
finding the minimum cardinality consistent set of prototypes, [117], i.e., a set of prototypes
correctly classifying the whole training set $I$, is an NP-hard problem, [237]. Moreover, finding the subset of prototypes of given cardinality minimizing the number of misclassified objects is also shown to be NP-hard, [50]. Integer Programming formulations are proposed in [50] for selecting prototypes in small-size data sets. In order to address larger data sets, different heuristics have been proposed, including variable neighborhood search [50], particle-swarms [182], tabu search [53] and genetic algorithms [138].

2.5 Classification Trees

Classification trees are very appealing due to their simplicity and interpretability, while delivering a reasonable accuracy. Very well-known implementations are Classification and Regression Trees (CART) [36] and C4.5 [197]. See [240] for a comparison and for the description of other tree-based methods.

A classification tree is a classifier defined as a series of if-then rules. For this reason, classification trees are considered to be the champions in terms of interpretability.

The classifier is identified with a rooted tree $T$, in which each node represents a partition of the space $X$. In the simplest case, $T$ is a binary tree, and each node represents a partition of $X$ into two sets of the form $\{x \in X : x_\ell \geq b\}$ and $\{x \in X : x_\ell < b\}$ for some variable $\ell$ and threshold $b$. The set $S$ of leaf nodes of $T$ then induces a partition $\{X_s : s \in S\}$ of $X$, and the classifier assigns to any $x \in X_s$ as label $y(x)$ the most frequent class in the training sample $I$ whose predictor vector belongs to $X_s$.

To construct the classifier, the topology of its associated rooted tree, as well as the splitting associated with each node, is to be defined. The choice of the topology is simplified if, as customary, trees are assumed to be binary trees. The tree is then constructed following a greedy procedure, in which new nodes are recursively created and connected with the previously defined nodes until a stopping criterion is defined. Therefore, to train a classification tree, we need to define a splitting criterion as well as a stopping criterion.

As we have said above, in the simplest case, nodes are split using a pair (variable, cutoff). The aim is to choose a pair such that the prediction accuracy improves. This is usually measured by node impurity. The classical examples of node impurity come from Information Theory, such
as the well-known Gini index and Entropy, proposed in the very early days. Since then, many other splitting criteria have been proposed, see [150] and references therein.

Univariate splits, i.e., splits defined by one variable, are intuitive, and therefore plausible, when interpretability is pursued. However, multivariate counterparts might be better in terms of accuracy [37, 180]. (Notice that, as pointed out in [19], multivariate decision trees are found in the literature with other names, such as oblique trees or perceptron trees.) The most popular multivariate splits are the linear ones. Apart from greedy and heuristic techniques, linear splits can be constructed using LDA [151], Linear Programming [21], Integer Programming [26] and linear SVMs [185], to name a few. This illustrates the central role Mathematical Optimization plays when deriving these (non)linear splits. Nonlinear multivariate splits are a real departure from interpretability, one of the main salient features of classification trees, and therefore less popular in the literature, [86].

In terms of stopping criteria, it is usual to require a minimum number of training objects in each leaf node. In practice the tree is pruned, yielding a subtree of the original one, and thus of reduced size.

With the aim of reducing the computational effort, enhancing interpretability and making the classifier more robust against outliers, one can, as a preprocessing step, discretize the variables, thus reducing the number of candidate values to be checked as potential cutoffs, [147]. The benefit of discretization is not only limited to classification trees. Indeed, discretization is also useful when the method in question can only handle binary data, which is the case, among others, of the Logical Analysis of Data. In this context, in [29], the authors explore several combinatorial optimization approaches for discretizing the variables, as well as their computational complexity. In [202], the classification accuracy of SVM with original data and data discretized by state-of-the-art discretization algorithms are compared on both small and large scale data sets. The computational results demonstrate that SVM with discretized data leads to similar and sometimes better accuracy than SVM with original data, while the corresponding optimization problem is significantly reduced in size.

The performance of a single classifier can be improved by ensembling classifiers, which are combined, for instance, by a voting process. See [80, 96] and references therein. This
strategy, applicable to any family of classifiers, has successfully been applied to classification
trees, under the names of boosting [95], bagging [34], random forests [35] and node harvest
[174]. Optimization has shown to be useful to decide how classifiers should be ensembled. For
instance, in [77, 206] a column generation approach, [105], is used in the boosting environment,
whereas a quadratic programming model is used in [174].

3 Support Vector Machines

3.1 Introduction

Quoting [240], SVM

is considered a must try -it offers one of the most robust and accurate methods
among all well-known algorithms. It has a sound theoretical foundation, requires
only a dozen examples for training, and is insensitive to the number of dimensions.
In addition, efficient methods for training SVM are also being developed at a fast
pace.

The origins of SVMs are found in the literature of Statistical Learning, where it is shown
that the probability of misclassifying a forthcoming individual can be bounded by a decreasing
function of the margin, this bound being independent of the data distribution, [231]. Moreover,
under mild conditions, the SVM solution approaches the optimal (Bayes) rule when the sample
size increases, [146].

In this paper we will discuss the 2-class problem and the geometrical interpretation of SVM
in this case. For more than two classes, different procedures exist to reduce the analysis to (a
series of) 2-class problems, as reviewed e.g. in [101, 120, 123, 198, 230, 233].

Suppose a 2-class problem. For a linear classifier, constructed from scoring functions \( f_{-1} = 0 \)
and \( f_1(x) = \omega^T x + \beta, \omega \neq 0 \), the polyhedra \( X_c \) defined in (4) are halfspaces whose common
boundary is the hyperplane \( \omega^T x + \beta = 0 \). In its simplest version, the so-called hard-margin, we
are given the training sample \( I \), and the hyperplane \( \omega^T x + \beta = 0 \) is sought such that no element
in the training sample \( I \) is misclassified, i.e., \( x^i \in \mathbf{X}_y, \forall i \in I \), and the minimum distance from
the points in the training sample to such hyperplane is maximized. Such a distance is called the margin, [30, 72, 229, 230], and thus the hard-margin SVM seeks the separating hyperplane with the largest margin.

In the following, we will present the hard-margin and the soft-margin approaches to SVM as distance-optimization problems. We will then model the case in which the data are embedded into a feature space of higher dimension, and then work out the so-called kernel trick, allowing us to build nonlinear classifiers.

3.2 Hard-margin approach

In the hard-margin approach, the training sample is assumed to be linearly separable, i.e., the convex hull of the two groups are not empty and they do not overlap, and it is imposed that all objects in the training sample must be correctly classified. The separating hyperplane is the one maximizing the smallest distance to misclassification, [70]. Let $\| \cdot \|$ be the norm used to measure the distance to hyperplanes in $\mathbb{R}^p$. Then, for any object $i \in I$ with $x^i \in X_{y^i}$, the distance of $x^i$ to the hyperplane $\omega^\top x + \beta = 0$ is given by

$$\frac{y^i (\omega^\top x^i + \beta)}{\|\omega\|^o},$$

[192], where $\| \cdot \|^o$ denotes the dual of $\| \cdot \|$, i.e., $\|\rho\|^o = \max \{ \rho^\top x : \|x\| = 1 \}$. Hence, $(\omega, \beta) \in \mathbb{R}^p \times \mathbb{R}, \omega \neq 0$ is found by solving the following Mathematical Optimization problem:

$$\maximize \min_{i \in I} \frac{y^i (\omega^\top x^i + \beta)}{\|\omega\|^o}$$

subject to

$$y^i (\omega^\top x^i + \beta) > 0 \quad i = 1, \ldots, |I|$$
$$\omega \in \mathbb{R}^p \setminus \{0\}$$
$$\beta \in \mathbb{R}.$$

We may observe that the function returning the minimal distance to the hyperplane $\omega^\top x + \beta = 0$, $\rho(\omega, \beta) := \min_{i \in I} \frac{y^i (\omega^\top x^i + \beta)}{\|\omega\|^o}$ is homogeneous, i.e.,

$$\rho(\delta \omega, \delta \beta) = \rho(\omega, \beta),$$
for any $\delta > 0$. Thus, without loss of optimality, we can replace constraint (6) with

$$y^i(\omega^\top \mathbf{x}^i + \beta) \geq 1 \quad i = 1, \ldots, |I|.$$  

With this tighter constraint, it is easy to see that the hard-margin model is equivalent to

$$\text{maximize} \quad \frac{1}{||\omega||^\circ}$$  

subject to

$$y^i(\omega^\top \mathbf{x}^i + \beta) \geq 1 \quad i = 1, \ldots, |I|$$

$$\omega \in \mathbb{R}^p \setminus \{0\}$$

$$\beta \in \mathbb{R},$$

which can be rewritten as the following minimization problem with convex objective and linear constraints:

$$\text{minimize} \quad ||\omega||^\circ$$

subject to

$$y^i(\omega^\top \mathbf{x}^i + \beta) \geq 1 \quad i = 1, \ldots, |I|$$

$$\omega \in \mathbb{R}^p$$

$$\beta \in \mathbb{R}.$$  

Observe that $\omega = 0$ does not give feasible solutions. Hence, there is no need to impose that $\omega \neq 0$, allowing one to write the feasible region as a closed (polyhedral) set.

Problem (7)-(10) can be rephrased in terms of the $\omega$ variables as finding the vector with minimum $||\cdot||^\circ$ norm in the polyhedron \{ $\omega : y^i(\omega^\top \mathbf{x}^i + \beta) \geq 1 \forall i \in I$, for some $\beta$ \}. Therefore an optimal $\omega^*$ always exists. Moreover, at least one constraint (8) must be active at optimality, forcing $\beta$ to have the form $y^i - (\omega^*)^\top \mathbf{x}^i$ for some $i \in I$. Uniqueness issues are more subtle, yet important: different optimal solutions may classify future objects differently. Uniqueness is guaranteed if $||\cdot||^\circ$ is a strictly convex norm [230], such as the $\ell_2$ norm, but not, for instance, for the $\ell_1$ norm.
Obviously the objective function (7) can be replaced by $\Psi(\|\omega\|)$ for any $\Psi$, increasing in $\mathbb{R}^+$. Usually, $\|\cdot\|$ is the Euclidean norm, and thus its dual norm too. In this case, taking $\Psi(t) = \frac{1}{2} t^2$, one obtains an equivalent formulation as a convex quadratic problem with linear constraints.

Clearly the hard-margin optimization problem may be infeasible, i.e., the two classes may not be linearly separable. This infeasibility can be handled in different ways, either by means of the soft-margin approach, as described in Section 3.3, or by embedding the data into a feature space of higher dimension, see Section 3.4. Note that these two approaches are not exclusive, and that they can be applied even if the data are linearly separable.

### 3.3 Soft-margin approach

When data are not linearly separable, Problem (7)-(10) is infeasible. In the soft-margin approach, constraints (8) are perturbed by introducing auxiliary variables $\xi^i$, making the new problem always feasible, [70].

The classifier is found by solving the following optimization problem:

\[
\text{minimize } \Psi(\|\omega\|) + \sum_{i=1}^{\lvert I \rvert} g_i(\xi^i)
\]

subject to

\[
y^i(\omega^\top x^i + \beta) \geq 1 - \xi^i \quad i = 1, \ldots, \lvert I \rvert \quad (12)
\]

\[\xi^i \geq 0 \quad i = 1, \ldots, \lvert I \rvert \quad (13)\]

\[\omega \in \mathbb{R}^p \quad (14)\]

\[\beta \in \mathbb{R} \quad (15)\]

where $\xi = (\xi^i) \in \mathbb{R}^{\lvert I \rvert}$ is the vector of deviation variables, and, for each $i \in I$, $g_i$, the loss function, is convex and increasing in $\mathbb{R}_+$. The most popular choices for the loss function are the so-called hinge loss, $g_i(t) = C_i t$ or the squared hinge loss, $g_i(t) = C_i t^2$.

Thus, a compromise between the norm of the normal vector of the hyperplane and the deviations, measured as the sum of the losses at the different objects, is sought.
Contrarily to what happens with the hard-margin problem, there is no guarantee that all points in $I$ are correctly classified by the optimal solution of Problem (11)-(15). The correct classification of objects in the training sample is given by the deviation variables. Indeed, an object $i \in I$ will be correctly classified if $0 \leq \xi^i < 1$, misclassified if $\xi^i > 1$, while for the case $\xi^i = 1$, we get a tie in expression (1). Therefore, $\sum_{i=1}^{\|I\|} \xi_i$ is an upper bound of the number of misclassified objects.

As in the hard-margin approach, the feasible region of the soft-margin model is polyhedral. However, uniqueness of the optimal solution calls for more restrictive assumptions than in the hard margin case. For instance, assuming $\Psi$ to be strictly convex and strictly increasing in $R_+$, and the norm $\| \cdot \|$ to be smooth, then uniqueness of the $\omega$ is guaranteed. See in [41] a simple example with $\ell_2$-SVM and multiple optimal classifiers.

It is also possible for Problem (11)-(15) to have $\omega = 0$ as optimal solution, implying that all objects are allocated to the very same class, or, if $\beta = 0$, all objects become unclassified according to (2).

With the usual choices of loss functions $g_i$, either $g_i(t) = C_i t$ or $g_i(t) = C_i t^2$, the soft-margin model can still be written as a convex quadratic problem with linear constraints. In general, and for any shape of the objective function, the soft-margin model can be transformed into an unconstrained problem, since at optimality each $\xi^i$ takes the value $(1 - y^i(\omega^\top x^i + \beta))^+$, where $(a)^+ = \max\{a, 0\}$. Thus one can reformulate Problem (11)-(15) as

$$
\text{minimize}_{\omega \in R^p, \beta \in R} \Psi(\|\omega\|^\circ) + \sum_{i=1}^{\|I\|} g_i((1 - y^i(\omega^\top x^i + \beta))^+).
$$

Expression (16) gives a different insight into the geometrical problem of maximizing the margin: we can see the problem as a regularization problem, in which a regularization term $\Psi(\|\omega\|^\circ)$ is added to the so-called empirical risk, i.e., the sum of losses in the data set. See e.g. [121].

Smoothing techniques to replace the non-smooth operator $(\cdot)^+$ by a smooth proxy are discussed in [142], whereas [166] rewrites (16), for the $\ell_1$ norm, as an equivalent unconstrained problem with smooth objective, solved via a Newton-type method. The problem above can also be successfully handled using non-smooth optimization methods. See for instance [211, 212] for a stochastic subgradient descent algorithm.
3.4 Mapping into a feature space: the kernel trick

Instead of applying the soft margin approach, as described in the previous section, to the crude data, better results may be obtained if data are first embedded into a feature space $V$ of higher dimension, equipped with a scalar product via a mapping $\phi : \mathbb{R}^p \to V$. Different popular choices for the mapping $\phi$ exist. One can take, for instance, polynomial functions, such as $\phi(x) = (x_1, x_2, \ldots, x_p, x_1^2, x_1 x_2, \ldots, x_p^2)$. In the so-called Binarized SVM, $[48]$, $\phi$ takes values in binary vectors in high dimension,

$$\phi(x) = (\varphi_{\ell,b}(x))_{\ell,b},$$

with $\varphi_{\ell,b}(x) = 1$ if $x_\ell \geq b$, and zero otherwise, for each $\ell = 1, \ldots, p$ and each $b$, midpoint of consecutive values of $x_\ell$ in the data set. In this way, the set of original variables is transformed into a large set of features, in which one checks whether a given variable $x_\ell$ takes a value higher than a certain threshold $b$.

Once the data have been transformed, the hyperplane $\omega^T \phi(x) + \beta = 0$ is found by solving the following optimization problem:

$$\text{minimize } \Psi(\|\omega\|^2) + \sum_{i=1}^{|I|} g_i(\xi^i)$$

subject to

$$y^i(\omega^T \phi(x^i)) + \beta \geq 1 - \xi^i \quad i = 1, \ldots, |I|$$

$$\xi^i \geq 0 \quad i = 1, \ldots, |I|$$

$$\omega \in V$$

$$\beta \in \mathbb{R}.$$ (22)

Observe that such inner product applies to data in the transformed space $V$, so we have a linear classifier in $V$ whereas we have a nonlinear discriminant function in the original input space.

Embedding the data set, via $\phi$, in a vector space of (much) higher dimension may considerably increase the size of the corresponding optimization problem. For instance, in the Binarized SVM a new feature is introduced for each variable $x_\ell$ and any possible midpoint $b$ between consecutive values of such variable in the sample training $I$. Taking as $\| \cdot \|$ the $\ell_1$ norm, $\Psi(t) = t$
and \( g(t) = C t \), Problem (18)–(22) is clearly a linear program with a large number of decision variables, solvable by a column generation approach.

When \( \| \cdot \| \) is the \( \ell_2 \) norm, \( \Psi(t) = \frac{1}{2} t^2 \) and \( g(t) = C t \), solving the dual of Problem (18)–(22) brings enormous computational advantages due to the so-called kernel trick. By constructing the Lagrangian function and imposing the optimality conditions, the dual of Problem (18)–(22) can be written as the following concave quadratic maximization problem with linear constraints:

\[
\text{maximize} \quad \sum_{i=1}^{|I|} \alpha^i - \frac{1}{2} \sum_{i=1}^{|I|} \sum_{j=1}^{|I|} \alpha^i \alpha^j y^i y^j \phi(x^i)^\top \phi(x^j) \\
\text{subject to} \quad \sum_{i=1}^{|I|} \alpha^i y^i = 0, \quad 0 \leq \alpha^i \leq C_i = 1, \ldots, |I|,
\]

where \( \alpha = (\alpha^i) \in \mathbb{R}^{|I|} \) is the vector of dual variables to constraints (19).

Since classification takes involves the primal variables \( \omega, \beta \), one needs to know how to recover primal optimal solutions from a dual optimal solution. From Karush–Kuhn–Tucker (KKT) conditions one obtains an expression for the optimal \( \omega \) as

\[
\omega = \sum_{i=1}^{|I|} \alpha^i y^i \phi(x^i),
\]

thus \( \omega \) belongs to the vector space spanned by the (transformed) vectors. Only those \( i \in I \) with strictly positive multiplier \( \alpha^i \) play any role, and they are called the support vectors, the remaining objects being irrelevant for classification purposes. In other words, the SVM performs a prototype selection, as described in Section 2.4 for Nearest Neighbor methods. However, in this case there is no limit on the number of prototypes to be selected, which will be given by the algorithm. This number may be very large, since, as shown in [219], the number of support vectors may grow linearly in the number of data points.

Complementarity slackness conditions also imply that, for any \( i \in I \) with \( 0 < \alpha^i < C \), one has \( y^i (\omega^\top \phi(x^i) + \beta) = 1 \), and therefore object \( i \) is, after embedding via \( \phi \), on the hyperplane \( y^i (\omega^\top z + \beta) = 1 \), which is parallel to the separating hyperplane in \( V \). In particular, one can obtain \( \beta \) from any such \( i \in I \) as \( \beta = y^i - \omega^\top \phi(x^i) \).
When no \( i \in I \) exists with \( 0 < \alpha^i < C \), different arguments can be used to obtain \( \beta \), [41].

First, \( \omega \) is obtained from the dual formulation by (26), and then \( \beta \) is found by solving the one-dimensional problem (16) for \( \omega \) fixed. Except for this pathological degenerate case, \( \beta \) can then be recovered from the dual as described above, and then the score at any \( x \) is given by

\[
\omega^\top \phi(x) + \beta = \sum_{i=1}^{\|I\|} \alpha^i y^i \phi(x^i)^\top \phi(x) + \beta. \quad (27)
\]

Given the mapping function \( \phi \), we can define its corresponding kernel as \( K : \mathbb{R}^p \times \mathbb{R}^p \rightarrow \mathbb{R} \), where \( K(x, z) = \phi(x)^\top \phi(z) \). The objective function of the dual problem (23)–(25) can be now written in terms of the kernel and the whole problem reads as follows

\[
\text{maximize } \sum_{i=1}^{\|I\|} \alpha^i - \frac{1}{2} \sum_{i=1}^{\|I\|} \sum_{j=1}^{\|I\|} \alpha^i \alpha^j y^i y^j K(x^i, x^j). \quad (28)
\]

subject to

\[
\sum_{i=1}^{\|I\|} \alpha^i y^i = 0 \quad (29)
\]

\[
0 \leq \alpha^i \leq C \quad i = 1, \ldots, \|I\|. \quad (30)
\]

Model (28)–(30) is a quadratic concave problem, with \( \|I\| \) variables and only one linear constraint, and can be solved efficiently by standard techniques, see [72]. It is remarkable that explicit knowledge of \( \phi \) is not needed, since only the kernel induced by \( \phi \) appears in this formulation. Moreover, evaluating forthcoming data does not require either the explicit use of \( \phi \), since, once \( \alpha \) is obtained as optimal solution to the dual, and \( \beta \) is obtained from complementarity slackness conditions, (27) is re-written as

\[
\omega^\top \phi(x) + \beta = \sum_{i=1}^{\|I\|} \alpha^i y^i K(x^i, x) + \beta. \quad (31)
\]

This implies that one can work directly with the kernel function \( K \) without explicit use of the embedding function \( \phi \).

Taking as \( \phi \) the identity, we get the linear kernel,

\[
K(x, z) = x^\top z. \quad (32)
\]
One of the most popular kernels is the so-called Radial Basis Function (RBF), defined as

\[ K(x, z) = \exp(-\|x - z\|^2/\gamma), \]  

(33)

where \( \gamma \) is a parameter. Other standard kernels are based on polynomial or sigmoidal functions, see [72, 123, 124] and the references therein. In [139], it has been acknowledged that heterogeneous data call for multiple-kernel learning, i.e., a convex combination of kernels.

Intuitively, \( K \) plays the role of a similarity measure between objects. This is evident for the kernel given in (33). For the linear kernel, given in (32), take \( K^\ast(x, z) = -\frac{1}{2} \|x - z\|^2 = K(x, z) - \frac{\|x\|^2}{2} - \frac{\|z\|^2}{2} \). Constraint (29) implies that, for any dual feasible solution, the objective in (28) with \( K^\ast \) is identical to the objective with \( K \). In other words, the duals with \( K \) and \( K^\ast \) are identical, showing that the linear kernel \( K \) can also be seen as the standard similarity measure in IR^p.

By construction, the kernel matrix \( (K(x^i, x^j))_{i,j\in I} \) is symmetric and positive semidefinite. However, many potential kernels, such as those found in [172, 207, 215], violate such assumptions. When positive semidefiniteness is lost, Problem (28)–(30) is not a concave maximization problem any more, and new optimization approaches are needed, e.g. [111, 157, 156].

It is worth mentioning that the paradigm of kernels is not reduced to classification problems with data in IR^p. Indeed, different authors have proposed dissimilarity-inspired kernels in different contexts. See, for instance, [171] for a kernel in the space of variable-length amino acid sequences. Furthermore, kernels are not restricted to Supervised Classification problems, since the same idea has been proposed and successfully used for techniques such as clustering analysis, principal component analysis, etc. The reader is referred to [124] for a recent presentation of the state-of-the-art of the theory on kernel methods and applications.

As described above, the kernel trick is an extremely powerful tool, which has successfully been used in, among others, SVM. However, even though the usual is to work in the dual space, working with the primal problem (18)–(22) is receiving an increasing attention, [56, 132, 161, 223]. This may be useful if a reduced expression of \( \omega \) in terms of a set of functions \( \phi \) is sought, as in [131]. Moreover, many challenging problems have data sets with a very large number of objects, very sparse features, and a rich structure which may not be well captured if kernels are used. See e.g. [223] for some motivating examples.
3.5 Other norms to measure distance to hyperplanes

Distances to hyperplanes are usually assumed to be measured by the Euclidean distance, allowing for the kernel trick. This has two main consequences: the dimensionality of the resulting optimization problems does not depend on the original dimension of the data, making the technique useful for data sets in very large dimensions, and, besides, with an appropriate choice of the kernel, many different classification problems, not necessarily with predictor vectors in the Euclidean space, can be considered.

In spite of the benefits of modeling distances to hyperplanes with the Euclidean distance, several authors have proposed the use of other distance measures [47, 48, 149, 163, 191, 247], mainly the $\ell_1$ norm. In this way, linear, instead of quadratic, optimization problems are obtained, making, in principle, possible to handle problems with much larger data sets. Moreover, it is frequently advocated that $\ell_1$-SVM methods tend to generate sparse classifiers, i.e., just a few variables are retained, which may be a valuable information to understand how the classifier behaves.

In any case, using norms (thus convex functions) to measure distances, make the resulting margin-maximization problem a convex problem, thus we have nothing to worry about getting stuck at a local optimum, in contrast with what happens with other classification procedures.

3.6 Departing from convexity in SVM

An assumption made so far on the loss functions $g_i$ in (11) is convexity, making (11)-(15) a (possibly smooth) convex optimization problem. However, different authors have advocated, using different arguments, for aggregating the deviations $\xi^i$ via nonconvex loss functions.

Outliers are observations which are far from their own class in the feature space, having therefore a large deviation $\xi^i$. Since misclassification error is measured by the surrogate $\sum_{i=1}^{[T]} \xi^i$, outliers will affect the location of the separating hyperplane and therefore the prediction accuracy in new objects. To overcome this, the so-called ramp loss has been proposed. Deviations $\xi^i$ are truncated avoiding extreme values, replacing then the hinge loss by a piecewise linear continuous function, constant from a given deviation on. Thus, a classifier more robust against outliers is obtained, [241]. In [38], a nonlinear mixed-integer formulation of the SVM with ramp
loss is proposed, where a binary variable is introduced for each training object equal to 1 if the
object is misclassified outside the margin and 0 otherwise. The ramp loss has also been advo-
cated in [213, 66] with the motivation of generating less support vectors than the SVM with
hinge loss. The objective is written as the difference of two convex functions and a local-search
procedure called CCCP, [244], is proposed. CCCP, a primal variant of the primal-dual DCA of
[3], optimizes a series of convex overestimates of the objective, obtained by linearizing one of
the terms in its decomposition as difference of two convex functions.

Discontinuous loss functions $g_i$ have been proposed in [38, 148, 186]. With the big $M$ trick,
linear (for the $\ell_1$-SVM) or quadratic (for the $\ell_2$-SVM) mixed-integer programs are solved using
general-purpose software or heuristic approaches.

3.7 Related distance-based approaches

Although SVM in the form presented above is by far the most popular distance-based linear
classification method, other related approaches have been proposed in the literature.

Among others, it is worthwhile mentioning the so-called Least Squares SVM proposed in
[104, 221] and the Proximal Support Vector Machine in [98, 101]. In both cases, inequality (19)
must be satisfied without slack, and deviation variables $\xi^i$ are now free. Both models differ
in the objective function. In (18), they both take $\Psi(t) = \frac{1}{2} t^2$ and $g(t) = C^2 t$. However, the
objective in [98, 101] has an additional term, namely $\frac{1}{2} \beta^2$.

In short, both methods seek two parallel hyperplanes, each associated with one of the groups,
such that the points are clustered around their corresponding hyperplane. Now, solving KKT
conditions amounts to solving a system of linear equations, and the kernel trick applies.

In [160] a model is introduced for data sets which are not linearly separable. The classifier is
defined by the hyperplane minimizing the sum of the distances of the objects to their halfspace
of correct classification. In other words, one minimizes the sum of the perturbations on the
objects such that the perturbed set becomes linearly separable. This problem reduces to a
combinatorial optimization problem, [51], since it is shown that an optimal hyperplane contains
a full-dimensional subset of $I$. Hence, the search of an optimal hyperplane is reduced to
inspecting full-dimensional subsets of $I$. An exact method is proposed in [9], whereas VNS-
based heuristics have been given in [128, 194].

In [168], instead of maximizing the margin, the sum of reciprocal of the residuals is minimized, yielding second-order cone programs.

No matter which norm is used to measure distances, the idea of margin maximization always yields a linear classifier, since the boundary of the two classification regions is given by a hyperplane. Whereas nonlinear boundaries are obtained by using the kernel trick with a nonlinear kernel, an alternative approach is to construct classifiers whose classification regions are bounded by surfaces of predetermined shapes, such as piecewise linear regions, piecewise conic regions, spherical or ellipsoidal surfaces, e.g. [173, 12, 14, 15, 222, 85, 6, 8]. The resulting optimization problems have been addressed using Nonsmooth and Global Optimization techniques [7, 13].

4 Building an SVM classifier

The construction of the classifier is done following a bilevel process. In the inner level an optimization problem, usually in the dual form (28)–(30), or in the primal form (18)–(22) is addressed. All model parameters, including the kernel (or, in the primal version, the embedding $\phi$) as well as the loss functions, are assumed to be fixed. Different numerical methods and implementations will be reviewed in Section 4.1.

The outer level is a model selection step, in which a search in the parameter space is performed. Model selection approaches are reviewed in Section 4.2.

4.1 Training the SVM

Different general-purpose numerical methods have been proposed and customized to find the SVM classifiers. These include interior-point, active-set and (sub)gradient-type methods and they address either the dual or the primal programs mentioned above. When gauging the appropriateness of an algorithm, it should be taken into account that training is usually performed off-line, and thus speed may not be the main property sought.

Instead, the ability to address problems with large data sets, both in terms of number of data
and also dimensionality of the data, is a major concern, and standard optimization algorithms may become inefficient unless they conveniently exploit the problem structure. On the other hand, numerical accuracy of the algorithm, a major concern in Mathematical Optimization, may be a secondary objective in this context: the criterion to be optimized (the margin) is nothing but a surrogate of the ideal performance measure (probability of misclassification). Algorithms providing very quickly a reasonably good solution (and thus allowing one to test different parameters values) may be preferable to an algorithm focused in finding an $\varepsilon$-optimal solution of an optimization problem which surrogates the minimization of the misclassification probability. In the numerical experiments reported in [223] it is concluded that, in general, the generalization improved as the approximation gap decreased, but such improvement in generalization became rather insignificant. See also [22, 211].

As we have seen above, training the SVM with Euclidean distances and hinge losses is equivalent to solving the dual problem (28)–(30). This is a quadratic programming problem, where the number of variables is equal to the number of training points, and the feasible region consists of a linear constraint as well as upper and lower bounds on the variables. Typically, this quadratic programming problem is solved using either interior point methods, e.g. [89, 239] or active-set methods, e.g. [30, 187, 195, 164].

Interior point methods address the linearly constrained quadratic problem by passing its (linear) constraints to the objective via a barrier function. In this way, the original problem is replaced by a series of unconstrained problems, which can be solved efficiently using Newton or Quasi-Newton methods.

Interior Point methods are known to provide excellent accuracy, at the price of run times and memory requirements which may be unacceptable for large data sets, and are more suitable for low-rank kernel matrices, [91], which is the case of the linear kernel.

In general, active-set approaches are probably the most popular when training SVMs and can be found implemented in some of the SVM packages, since they overcome the typical memory requirements of Interior Point methods, and can thus handle large data sets, as those found in many application fields. For a solution to the dual problem (28)–(30), the dual active set is the set of variables $\alpha^i$ which are either equal to 0 or $C$. An active-set approach starts with
a solution to the problem at hand, and moves iteratively to new solutions. The new solutions are obtained by solving the reduced dual problem defined by the so-called working set, a subset of variables which are not in the dual active set. In particular, the SMO, Sequential Minimal Optimization method by Platt [195] is one of the most well-known active-set approaches, in which the working set has cardinality two. SMO was subsequently improved in [135], and the convergence of this improvement was proved in [133]. Since then numerous papers have been devoted to active-set approaches, see e.g. [145, 155, 208, 226] and references therein.

Unconstrained (sub)gradient-type methods have also been proposed to solve the primal problem. For instance, the Pegasos algorithm, [211, 212], is a stochastic subgradient algorithm which generates at each step a sample of $k$ objects in the training sample to compute an approximate subgradient of the objective function of (16). These methods are known to exhibit slow convergence rates, but they are less demanding for high-dimensional problems.

See also [90] for semi-smooth methods and [238] for parallel implementations.

State-of-the-art software for SVM includes libraries such as LIBSVM [54], SVMTorch [64] and SVMlight [127]. Moreover, more general-purpose numerical, statistical and Machine Learning packages such as MATLAB, R, SAS and WEKA [234], have also subroutines to train SVMs.

### 4.2 Model selection

Classifiers usually depend on some parameters. Since such parameters can affect the performance of the resulting classifier, parameter tuning becomes crucial. Indeed, it is pointed out in [140] that empirical evidence suggests that parameter tuning is often more important than the choice of algorithm, SVM being harder to tune than other classification procedures.

When training a SVM, one of the critical elements to be tuned is the trading parameter $C$. Another element subject to tuning is the kernel. There, we can choose the parameters of a given kernel, such as $\gamma$ in the RBF kernel, but we can also tune the kernel coefficients when a multiple kernel learning is pursued. In [149], the $|| \cdot ||^\circ$ norm is modeled as an $\ell_p$ norm and the tuning of the parameter $p$ is proposed.

In [118], it is observed that the optimal dual multipliers $\alpha_j$ are piecewise linear in the parameter $C$, allowing for a description of the full path of optimal classifiers when $C$ varies. In
[134], the asymptotic behavior of the SVM classifier for extreme values of $C$ and $\gamma$ is analyzed, characterizing cases for which the classifier underfits or overfits the data. However, both results do not directly extend to the case of more parameters. In any case, in practice, one single classifier is sought. Choosing the parameters with the best performance in terms of classification of forthcoming individuals, i.e. the so-called model selection problem, is an ill-defined problem, since the distribution of such individuals is unknown. Hence, surrogates are used, and one seeks the parameters optimizing either a lower bound of the probability of correct classification, [59, 130], or an estimate of accuracy, such as the crossvalidation error estimate, [136]. See [83] for a comparison of the performance of crossvalidation against that of several error bounds.

In both surrogate approaches, the model selection problem can be formulated as a bilevel programming problem, where in the inner problem we train a SVM model for a given choice of the parameters, while the objective function of the outer problem is equal to the surrogate described above. However, only recently the problem has been addressed as such, [137].

Optimizing bounds is suggested in [59, 130]. In [59] various bounds on the probability of misclassification are suggested, such as the support vector count or the radius-margin bound, as the objective function to be minimized. As a first step, strategies to smooth these bounds are proposed. An alternating procedure is presented, in which one alternates steps of finding the optimal SVM for a given choice of the parameters and then uses a gradient descent method to optimize the parameters for a given choice of the SVM, i.e., developing a greedy approach to solve the bilevel programming problem. In [130], the focus is on the radius-margin bound.

If $k$-fold crossvalidation is used, the parameter selection problem is written as a (global) optimization problem of the form

$$\max_{\vartheta} \frac{1}{k} \sum_{j=1}^{k} a_j(\vartheta),$$

(34)

where $a_j(\vartheta)$ is the accuracy measure evaluated if the model parameter is $\vartheta$ and the classifier is constructed from sample $I \setminus I_j$ and tested on sample $I_j$, $I_1, \ldots, I_k$ being the $k$ folds. Observe that the objective function in (34) is piecewise constant if accuracy $a$ is measured by the fraction of correctly classified individuals in the testing set. It is usual to solve (34) by using a grid search. This approach is therefore computationally demanding, mainly when several parameters are to be tuned. In order to alleviate the computational burden of grid search, different strategies
have been proposed. These include pattern search methods, [178] or evolutionary algorithms, [63, 97, 152].

Whereas the standard model selection is reduced to (approximately) finding the optimal parameter $C$ and at most a few more parameters of the kernel, in more recent research the kernel to be used is assumed to be a decision variable too, yielding the so-called kernel learning problem. In [139], the set $\mathcal{K}$ of feasible kernels is the set of symmetric positive-semidefinite matrices, and the optimal kernel can be found by solving a standard semidefinite programming problem, see also [67]. More tractable programs are obtained when the class $\mathcal{K}$ of kernels under consideration is further restricted. For instance, for $\mathcal{K}$ taken as the set of convex combinations of $m$ given kernels, [10] gives an adaptation of SMO, while in [217] the problem is formulated as a semi-infinite linear program and solved via column generation. In [82], choosing the optimal value of a kernel parameter is formulated as a bilevel programming problem.

5 Critical modeling issues

This section is devoted to discuss in detail critical modeling issues appearing in different contexts. We describe some models proposed in the literature addressing these issues and the Mathematical Optimization tools used to solve them.

5.1 Relevance of objects and classes

We have assumed so far that the accuracy of the classifier is measured through the probability of misclassifying forthcoming objects. However, in many applications, misclassifying individuals from different classes may have very different consequences. For instance, in credit management if a bank classifies as risky and denies a credit to a reliable firm, the bank may lose a customer; if, on the contrary, it gives credit to an unreliable customer, the credit money may not be returned. Similar examples can be given in the context of medical diagnoses and service booking cancelations, among others.

It may also be possible that data sets are unbalanced in terms of class sizes: the frequency of objects in the different classes in the data set $I$ may be rather different than the classes
frequencies of forthcoming objects.

A straightforward approach to cope with these situations is to introduce weights on training objects, indicating their relevance or prior probability, and solve then a weighted version of the standard SVM.

Weights on objects are also helpful when dealing with time series data, where usually more relevance is given to recent data, [42].

For problems in which misclassification errors in the two classes are not equally important, the standard approach consists of first calculating the optimal vector $\omega$, e.g. by solving the dual and then using a different criterion to choose the $\beta$. One can take $\beta$, for instance, so that the fraction of misclassified elements in class 1 is a given value.

An alternative way of dealing with unbalanced classes is to model the margin in a class, i.e., the margin between the separating hyperplane and the class [46]. The aim is therefore to maximize both margins, which yields a biobjective problem. In [46], it is shown that the Pareto-optimal solutions are hyperplanes parallel to the one obtained from the standard SVM model. Hence, it is sufficient to find the optimal normal vector $\omega$, which, as pointed out in Section 2.1, ranks the objects according to how likely is that they belong to class 1, and then the threshold value $\beta$ is chosen by taking into consideration the eventual imbalance of the classes. In this sense, the ROC curve, representing, for the different values of $\beta$, the fraction of misclassified points in both classes, is a valuable tool.

See [52, 196] for different proposals and an empirical comparison of different criteria.

### 5.2 Relevance of features

In some applications the amount of features is huge and training SVM using the entire feature set would be computationally very expensive, while its outcome would lack from insight. This is, for instance, the case in gene expression and text categorization.

One possible way to reduce problem dimensionality is to project the original data in an appropriate way via a function $\phi$, but contrarily to the aim in Section 3.4, we seek now a projection into a lower-dimensional space. One can then use standard statistical analysis projections techniques, such as (Kernel) Principal Component Analysis, [209], or adapt such projection
techniques to take into account that points are labeled, as e.g. in [193].

One may use as $\phi$ the projection onto a small subset of Cartesian coordinates, fully ignoring the remaining variables, considered to have little added value for classification. In this way, one obtains sparse classifiers, i.e., classifiers involving a reduced set of features, which is expected to be easier to interpret and also easier to evaluate. It is also widely accepted that working with a selected set of features can reduce dimensionality and the risk of overfitting, and improve the classification performance, [110, 109, 202].

One then faces the feature selection problem, i.e., the combinatorial problem of selecting a best-possible set of features, discarding the remaining ones. A vast amount of literature has been devoted to specific feature selection techniques, see [109, 183, 236] and references therein. Feature selection approaches are usually categorized as filters, wrappers and embedded. Filtering is performed as a preprocessing step prior to building the classifier, where the relevance of each feature is measured in the training data by a performance metric, such as, for instance the Pearson correlation coefficient or the Fisher criterion score. Features with a low score will be deleted from further analysis. Wrappers and embedded approaches are, in general, more successful but also computationally more costly. Wrappers are linked to a classification algorithm and its performance, usually its classification accuracy. Wrappers aim at selecting the best subset of features in terms of model performance. Finally, in an embedded approach the classification algorithm and the feature selection approach are difficult to separate. Feature selection is performed at the same time the classifier is being built. One of the most cited feature selection approaches is the recursive feature elimination algorithm for SVMs proposed in [110], a greedy method where the SVM classifier is built and the feature with the smallest absolute value of the coefficient in the separating hyperplane is discarded. This process is repeated until the number of features is below a given maximum.

Instead of selecting a subset of features, sparse classifiers can also be obtained by choosing appropriately $\| \cdot \|_{\circ}$. It is common knowledge that the $\ell_1$ norm yield, in general, sparse SVM classifiers, [100]. Another alternative is to use the so-called zero norm, $\| \omega \|_0 = |\{ i : \omega_i \neq 0 \}|$. (Note however that $\| \cdot \|_0$ is not a norm because the triangle inequality does not hold.)

The minimization of the zero-norm over a polyhedral set is an NP-Hard problem [2].
To make the problem tractable and, since the zero norm is a stepwise function, continuous, differentiable and concave approximations have been proposed to deal with the problem, [33, 199, 200, 235].

In between, one can consider the so-called $\ell_p$ norms, for $0 < p < 1$, [149], yielding a Global Optimization problem for tuning $p$.

5.3 Interpretablity and comprehensibility

SVM is a very competitive classification method in terms of accuracy due to the embedding of the data, yielding nonlinear classifiers fitting better the data. However, this embedding implies the departure from the original data, and the classifiers are constructed using transformed data. This transformation makes SVM classifiers less intuitive to users. This is critical when kernels are used without an explicit knowledge of the embedding function $\phi$ in Section 3.4 being used: solving the dual formulation (28)–(30) yields the support vectors, but this, as already pointed out in [18], provides little insight.

The type of classification rule used by SVM also undermines its intuitiveness. SVM constructs a separating hyperplane in the input space (or the transformed one) as a decision rule to classify new objects, instead of more intuitive counterparts such as classification trees, which are based on if-then rules.

These two issues make straight SVMs less appealing to practitioners in applications such as, for instance, credit scoring, medical diagnosis and marketing. As pointed out in [170], in credit scoring “when credit has been denied to a customer, the Equal Credit Opportunity Act of the US requires that the financial institution provides specific reasons why the application was rejected; indefinite and vague reasons for denial are illegal.” In medical diagnosis, physicians aim at interpreting the outcome of the classifier, and are less inclined to use black-box classifiers. In marketing, simple discriminant rules are sought for targeting campaigns. As said in Section 5.2, interpretability of the SVM classifier can be improved by performing feature selection. In the following, we discuss more specific approaches to improve interpretability.

For practitioners, if-then rules are more appealing, where the interpretability is granted. Therefore, in order to improve the interpretability/comprehensibility of the SVM classifier there
is an obvious alternative: extract if-then rules from SVMs, see [170] and references therein. A typical way of extracting an if-then rule from SVM would consist of the following steps: (1) train the SVM, (2) change the labels of the objects to the labels predicted by SVM and (3) derive an intuitive classification rule using the data with the SVM labels. To perform the third step, we can simply use C4.5, or any other classification tree. In the process of building this tree, the number of training observations at some of the nodes may be too low to derive new splits or to assign a class. Therefore, an additional step is sometimes performed, in which new training objects are artificially generated and labeled by SVM. At a possible loss of accuracy, we can therefore improve interpretability by generating a classification tree that resembles the SVM output.

Other rule extraction techniques have been proposed in [16, 79, 169, 184].

In the pursuit of interpretability, the so-called Binarized SVM introduced in [48] is trained with features of the form $\phi_{\ell,b}$ as defined in (17). The obtained classifier has several advantages. First, each of the features is simple and easy to interpret. Second, only some of these features will play a role in the final classifier, i.e., the corresponding weight will be different from zero. The cutoffs $b$ with nonzero weight can be seen as critical values to classification. Third, features with no critical values can be deemed as irrelevant. Fourth, by focusing on a given predictor variable, the weights of the corresponding critical values can be used to plot a stepwise function that models how the variable influences the classifier. This approach has been extended to detect not only relevant variables but also relevant interactions between variables to classification [49]. Other approaches to generate comprehensible models are, among others, inverse classification [167] and sensitivity analysis [243].

5.4 Costs on variables and/or features

In Sections 5.2 and 5.3, we have already argued the desirability of having a small number of active features in the SVM classifier, i.e., features having a weight different from zero in the separating hyperplane. Costs associated with variables and/or features is another reason for keeping down the number of active features.

The information recorded in the variables and/or the features may be the result of a test,
and thus having a monetary cost attached. Such a cost makes some features less attractive than others. Similarly, features requiring high computational costs are less attractive. Therefore, it may be desirable to assign costs to features to discriminate among them [227].

Some of the feature selection approaches in Section 5.2 can be seen as models including feature costs. However these costs are not discriminatory. In [47], the SVM is modified to include general costs on features. The aim is to minimize both misclassification rate and total feature costs, where a biobjective mixed-integer linear programming problem is addressed, yielding an approximation to the set of Pareto-optimal classifiers.

5.5 Imprecise data

SVM models can also be used to classify data affected by some kind of noise or perturbation, such as measurement errors. SVM classifiers dealing with imprecise data have been proposed in [224, 225]. Linear and second order cone programs are formulated and solved by interior point methods. These models are generalized in [45] by assuming that objects are not any more points in $\mathbb{R}^p$, but convex compact sets, such as rectangles. The soft margin approach is extended to this new context, by seeking a hyperplane separating the convex compact sets instead of single points.

In [1, 214], data in the two groups are assumed to be given by random variables, with known mean and covariance matrices. A quadratic chance-constrained programming problem is posed, by minimizing the norm of the normal vector $\omega$ and keeping the misclassification probability bounded. Using standard bounds for probabilities, the problem is rewritten as a second-order cone programming problem, and solved with interior point algorithms.

A different perspective is presented in [76]. It is assumed that data become corrupted during the classification phase, the subset of deleted and corrupted features being controlled by an adversary, and may vary from instance to instance. Following a worst-case approach, the risk of the classifier is measured by the fraction of objects which would be misclassified if a given fraction of features becomes corrupted (and thus unused). A linear programming formulation similar to the soft margin SVM is proposed, taking as $\| \cdot \|_\infty$ the $\ell_\infty$ norm.
5.6 Unlabeled data

In Data Mining, the motto is that there is an abundance of data available to us. However, the readiness of the class label is another matter. On one hand, this label may need to be obtained manually, such as in text categorization or junk mail classification. On the other hand, obtaining the label may imply expensive test costs, such as in medical applications. In this context, the semi-supervised SVM (S\textsuperscript{3}VM) has been proposed, in which the SVM is trained using both labeled and unlabeled data, [20], with the implicit assumption that objects which are close to each other in the feature space should have the same label. S\textsuperscript{3}VM is an extension of SVM since a maximum-margin separating hyperplane is sought, but now the labels of some objects in the training set are decision variables. Not only this increases the dimensionality of the optimization problem, but also convexity is lost. Indeed, one can either introduce boolean decision variables for the labels of the unlabeled objects, and thus one obtains a mixed-integer nonlinear problem, or, instead, one forces that all unlabeled points are far from the separating hyperplane: For each unlabeled training object \(i\), auxiliary deviations \(\xi_i^1, \xi_i^{-1}\) for the two classes, and the deviation associated with such object is defined as \(\xi^i = \min\{\xi_i^1, \xi_i^{-1}\}\). Adding this term to the objective function in the SVM yields a continuous optimization problem, now with a non-convex objective. Several methods have been proposed to address this problem, as reviewed in [58], either exact or heuristic. In the first class one finds [20, 57], in which binary variables are used for labeling the unlabeled objects. In [20] the \(\ell_1\) norm is chosen as \(\|\cdot\|\circ\), and, using the big \(M\) trick, a mixed-integer linear problem is obtained and solved with standard commercial software. In [57], the problem is written as the nonlinear problem in boolean variables \(y\) (the labeling variables) which gives, for each \(y\) the maximal margin if the unlabeled objects are labeled according to \(y\). Bounds are easily obtained from the SVM dual considering only the objects with labels known or fixed in the branch and bound tree.

The experimental results reported suggest that the globally optimal solution can return excellent generalization performance. Unfortunately, this approach is computationally demanding when the set of unlabeled data is large, [99].

The range of heuristics proposed is very wide. The experiments reported in [58] show that no algorithm clearly outperforms the others. In [65], a global optimization problem in
continuous variables is given. The objective function is written as a difference of two convex functions, and a local-search procedure is then designed by successively replacing the objective by a convex underestimate. Local-exchange methods, deterministic annealing methods and convex relaxations are also reviewed in [58].

5.7 Accommodating prior knowledge

In the SVM model, expressed as the optimization problem (11)-(15), no constraints are imposed on $\omega$ and $\beta$. However, in some occasions, some prior knowledge exists on the classifier one is willing to obtain, and such knowledge can be modeled as additional constraints on the decision variables.

For instance, [162] considers the problem in which prior expert experience, modeled as logical implications, is given. Assuming that the logical implications define polyhedral regions, these linear constraints are added to Problem (11)-(15). Using the $\ell_1$-SVM, the resulting problem is written in [162] as a semi-infinite linear program and as a linear program with equilibrium constraints, transformed into a simple linear program.

In the same vein, a ranking problem is addressed in [43]. A partial reflexive binary relation $\preceq$ on the set $X \subset \mathbb{R}^p$ is given, and a linear function $f$ on $\mathbb{R}^p$ of the form $f(x) = \omega^\top x$ is sought, so that the total order $\preceq^*$ induced by $f$,

$$x \preceq^* x' \text{ iff } \omega^\top x \leq (\omega^*)^\top x',$$

is compatible with $\preceq$, and given bounds on the relative importance of the different coordinates of $\omega$ are given. This problem is written as a 2-class classification problem, with objects in $X \times X$, training set $\{((x, x'), 1) : x \preceq^* x'\} \cup \{((x', x), -1) : x \preceq^* x'\}$, and the constraints on $\omega$ (the weights in the utility function) included in the SVM model.

It should be acknowledged that the inclusion of constraints in the primal SVM (11)-(15) may perturb the structure of both the primal and the dual, and thus an expression like (26) may not hold, avoiding the possibility of using the kernel trick.
6 Conclusions

In this paper we have described different bridges linking Mathematical Optimization with an active branch of Data Mining, namely, Supervised Classification. Special focus has been made on Support Vector Machines, SVM, an off-the-shelf procedure with deep theoretical properties and excellent empirical behavior as well. In its basic version, SVM calls for solving a convex quadratic problem with linear constraints. Critical issues in SVM, such as the detection of relevant features or the accommodation of measurement costs associated with the variables have been discussed, describing how Mathematical Optimization has been used to address such issues.

Convex Analysis plays a central role. However, techniques and algorithms from many different domains have also proved to be extremely successful. These include Integer Programming, Global Optimization, Linear Programming and Multiple-Objective Optimization. However, these techniques are usually seen with different eyes than in the Mathematical Optimization literature: the ability to solve large-scale problems, or the speed at which a good feasible solution is obtained may be much more important than convergence to an ε-optimal solution for very small ε.

The importance of Mathematical Optimization within Data Mining is not restricted to Supervised Classification. Indeed, other fields such as Unsupervised Classification (Cluster Analysis) or Regression, [216], also offer excellent opportunities for researchers in Mathematical Optimization. In particular, a large part of the methods and algorithms described in this paper have an equally successful counterpart in Regression Problems.

References


46


53
[199] F. Rinaldi, F. Schoen, and M. Sciandrone. Concave programming for minimizing the zero-

[200] F. Rinaldi and M. Sciandrone. Feature selection combining linear support vector machines

[201] B.D. Ripley. *Pattern Recognition and Neural Networks*. Cambridge University Press,
Cambridge, UK, 1996.

forecasting in revenue management. Working Paper, Saïd Business School, University of

[203] D. Romero Morales and J. Wang. Forecasting cancellation rates for services booking

[204] F. Rosenblatt. *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mech-

[205] P.A. Rubin. A comparison of linear programming and parametric approaches to the

89, 2009.

[207] H. Saigo, J.P. Vert, N. Ueda, and T. Akutsu. Protein homology detection using string

[208] K. Scheinberg. An efficient implementation of an active set method for SVMs. *Journal


