An Introduction to Kernel-Based Learning Algorithms

Klaus-Robert Müller, Sebastian Mika, Gunnar Rätsch, Koji Tsuda, Bernhard Schölkopf

Abstract—This review provides an introduction to Support Vector Machines, Kernel Fisher Discriminant analysis and Kernel PCA, as examples for successful kernel based learning methods. We first give a short background about VC theory and kernel feature spaces and then proceed to kernel based learning in supervised and unsupervised scenarios including practical and algorithmic considerations. We illustrate the usefulness of kernel algorithms by finally discussing applications such as OCR and DNA analysis.

Keywords—Kernel methods, Support Vector Machines, Fisher’s discriminant, Mathematical Programming Machines, PCA, Kernel PCA, single-class classification, Boosting, Mercer Kernels.

I. INTRODUCTION

In the last years, a number of powerful kernel-based learning machines, e.g., Support Vector Machines (SVMs) [1], [2], [3], [4], [5], [6], Kernel Fisher Discriminant (KFD) [7], [8], [9], [10] and Kernel Principal Component Analysis (KPCA) [11], [12], [13], have been proposed. These approaches have shown practical relevance not only for classification and regression problems but also, more recently, in unsupervised learning [11], [12], [13], [14], [15]. Successful applications of kernel based algorithms have been reported for various fields, for instance in the context of optical pattern and object recognition [16], [17], [18], [19], [20], text categorization [21], [22], [23], time-series prediction [24], [25], [19], gene expression profile analysis [26], [27], DNA and protein analysis [28], [29], [30] and many more.

The present review introduces the main ideas of kernel algorithms, and reports applications from OCR (optical character recognition) and DNA analysis. We do not attempt a full treatment of all available literature, rather, we present a somewhat biased point of view illustrating the main ideas by drawing mainly from the work of the authors and providing – to the best of our knowledge – reference to related work for further reading. We hope that new, nevertheless will be useful for the reader. It differs from other reviews, such as the ones of [3], [32], [6], [33], [34], mainly in the choice of the presented material: we place more emphasis on kernel PCA, kernel Fisher discriminants, and on connections to Boosting.

We start by presenting some basic concepts of learning theory in Section II. Then we introduce the idea of kernel feature spaces (Section III) and the original SVM approach, its implementation and some variants. Subsequently we discuss other kernel-based methods for supervised and unsupervised learning in Sections IV and V. Some attention will be devoted to questions of model selection (Section VI), i.e., how to properly choose the parameters in SVMs and other kernel-based approaches. Finally, we describe several recent and interesting applications in Section VII and conclude.

Table I Notation conventions used in this paper

| i, n | counter and number of patterns |
| X, N | the input space, N = dim(X) |
| x, y | a training pattern and the label |
| (x · x') | scalar product between x and x' |
| F | feature space |
| Φ | the mapping Φ : X → F |
| k(·, ·) | scalar product in feature space F |
| F_i | a function class |
| h | the VC dimension of a function class |
| d | the degree of a polynomial |
| w | normal vector of a hyperplane |
| α_i | Lagrange multiplier/Expansion coefficient for w |
| ξ_i | the “slack-variable” for pattern x_i |
| ν | the quantile parameter (determines the number of outliers) |
| ∥·∥_p | the l_p-norm, p ∈ [1, ∞] |
| | number of elements in a set S |
| Θ | The Heaviside function: Θ(z) = 0 for z < 0, Θ(z) = 1 otherwise |
| R_+ | space of non-negative real numbers |

II. LEARNING TO CLASSIFY — SOME THEORETICAL BACKGROUND

Let us start with a general notion of the learning problem that we consider in this paper. The task of classification is to find a rule, which, based on external observations, assigns an object to one of several classes. In the simplest case there are only two different classes.
possible formalization of this task is to estimate a function \( f : \mathbb{R}^N \to \{-1, +1\} \), using input-output training data pairs generated i.i.d. according to an unknown probability distribution \( P(x, y) \)

\[
(x_1, y_1), \ldots, (x_n, y_n) \in \mathbb{R}^N \times Y, \ Y = \{-1, +1\}
\]
such that \( f \) will correctly classify unseen examples \((x, y)\). An example is assigned to the class \(+1\) if \( f(x) \geq 0 \) and to the class \(-1\) otherwise. The test examples are assumed to be generated from the same probability distribution \( P(x, y) \) as the training data. The best function \( f \) that one can obtain is the one minimizing the expected error (risk)

\[
R[f] = \int l(f(x), y) dP(x, y),
\]

where \( l \) denotes a suitably chosen loss function, e.g. \( l(f(x), y) = \Theta(-y f(x)) \), where \( \Theta(z) = 0 \) for \( z < 0 \) and \( \Theta(z) = 1 \) otherwise (the so-called 0/1-loss). The same framework can be applied for regression problems, where \( y \in \mathbb{R} \). Here, the most common loss function is the squared loss: \( l(f(x), y) = (f(x) - y)^2 \); see [35, 36] for a discussion of other loss functions.

Unfortunately the risk cannot be minimized directly, since the underlying probability distribution \( P(x, y) \) is unknown. Therefore, we have to try to estimate a function that is close to the optimal one based on the available information, i.e. the training sample and properties of the function class \( F \) the solution \( f \) is chosen from. To this end, we need what is called an induction principle. A particular simple one consists in approximating the minimum of the risk (1) by the minimum of the empirical risk

\[
R_{emp}[f] = \frac{1}{n} \sum_{i=1}^{n} l(f(x_i), y_i).
\]

It is possible to give conditions on the learning machine which ensure that asymptotically (as \( n \to \infty \)), the empirical risk will converge towards the expected risk. However, for small sample sizes large deviations are possible and overfitting might occur (see Figure 1). Then a small

![Fig. 1. Illustration of the overfitting dilemma: Given only a small sample (left) either, the solid or the dashed hypothesis might be true, the dashed one being more complex, but also having a smaller training error. Only with a large sample we are able to see which decision reflects the true distribution more closely. If the dashed hypothesis is correct the solid would underfit (middle); if the solid were correct the dashed hypothesis would overfit (right).](image)

generalization error cannot be obtained by simply minimizing the training error (2). One way to avoid the overfitting dilemma is to restrict the complexity of the function class \( F \) that one chooses the function \( f \) from [3]. The intuition, which will be formalized in the following is that a "simple" (e.g. linear) function that explains most of the data is preferable to a complex one (Occam’s razor). Typically one introduces a regularization term (e.g. [37, 38, 39, 40]) to limit the complexity of the function class \( F \) from which the learning machine can choose. This raises the problem of model selection (e.g. [41, 39, 42, 43]), i.e. how to find the optimal complexity of the function (cf. Section VI).

A specific way of controlling the complexity of a function class is given by VC theory and the structural risk minimization (SRM) principle [44, 3, 5]. Here the concept of complexity is captured by the Vapnik-Chervonenkis (VC) dimension \( h \) of the function class \( F \) that the estimate \( f \) is chosen from. Roughly speaking, the VC dimension measures how many (training) points can be shattered (i.e. separated) for all possible labelings using functions of the class. Constructing a nested family of function classes \( F_1 \subset \cdots \subset F_k \) with non-decreasing VC dimension the SRM principle proceeds as follows: Let \( f_1, \ldots, f_k \) be the solutions of the empirical risk minimization (2) in the function classes \( F_i \). SRM chooses the function class \( F_j \) (and the function \( f_j \)) such that an upper bound on the generalization error is minimized which can be computed making use of theorems such as the following one (see also Figure 2):

**Theorem 1** ([3], [5]) Let \( h \) denote the VC dimension of the function class \( F \) and let \( R_{emp} \) be defined by (2) using the 0/1-loss. For all \( \delta > 0 \) and \( f \in F \) the inequality bounding the risk

\[
R[f] \leq R_{emp}[f] + \sqrt{\frac{h \ln \frac{2p}{\delta} + 1}{n} - \ln(\delta/4)}
\]

holds with probability of at least \( 1 - \delta \) for \( n > h \).

Note, this bound is only an example and similar formulations are available for other loss functions [5] and other complexity measures, e.g. entropy numbers [45]. Let us discuss Inequality (3): the goal is to minimize the generalization error \( R[f] \), which can be achieved by obtaining a small training error \( R_{emp}[f] \) while keeping the function class as small as possible. Two extremes arise for (3): (i) a very small function class (like \( F_1 \)) yields a vanishing square root term, but a large training error might remain, while (ii) a huge function class (like \( F_k \)) may give a vanishing empirical error but a large square root term. The best class is usually in between (cf. Figure 2), as one would like to obtain a function that explains the data quite well and at a small risk in obtaining that function. This is very much in analogy to the bias-variance dilemma scenario described for neural networks (see e.g. [46]).

### A. VC-dimension in practice

Unfortunately in practice the bound on the expected error in (3) is often neither easily computable nor very helpful. Typical problems are that the upper bound on the expected test error might be trivial (i.e. larger than one), the VC-dimension of the function class is unknown or it is infinite (in which case one would need an infinite amount of training data). Although there are different, usually tighter bounds, most of them suffer from similar problems. Nevertheless, bounds clearly offer helpful theoretical insights into the nature of learning problems.
Fig. 2. Schematic illustration of Eq. (3). The dotted line represents the training error (empirical risk), the dash-dotted line the upper bound on the complexity term (confidence). With higher complexity the empirical error decreases but the upper bound on the risk confidence becomes worse. For a certain complexity of the function class the best expected risk (solid line) is obtained. Thus, in practice the goal is to find the best tradeoff between empirical error and complexity.

B. Margins and VC-dimension

Let us for a moment assume that the training sample is separable by a hyperplane (see Figure 3), i.e. we choose functions of the form

\[ f(x) = (w \cdot x) + b. \tag{4} \]

It was shown (e.g. [44], [3]) that for the class of hyperplanes the VC-dimension itself can be bounded in terms of another quantity, the margin (also Figure 3). The margin is defined as the minimal distance of a sample to the decision surface. The margin in turn can be measured by the length of the weight vector \( w \) in (4): as we assumed that the training sample is separable we can rescale \( w \) and \( b \) such that the points closest to the hyperplane satisfy \( |(w \cdot x_i) + b| = 1 \) (i.e. obtain the so-called canonical representation of the hyperplane). Now consider two samples \( x_1 \) and \( x_2 \) from different classes with \( (w \cdot x_1) + b = 1 \) and \( (w \cdot x_2) + b = -1 \), respectively. Then the margin is given by the distance of these two points, measured perpendicular to the hyperplane, i.e. \( \left( \frac{w}{||w||} \cdot (x_1 - x_2) \right) = \frac{2}{||w||} \). The result linking the VC-dimension of the class of separating hyperplanes to the margin or the length of the weight vector \( w \) respectively is given by the following inequalities:

\[ h \leq \Lambda^2 R^2 + 1 \quad \text{and} \quad ||w|| \leq \Lambda \tag{5} \]

where \( R \) is the radius of the smallest ball around the data (e.g. [3]). Thus, if we bound the margin of a function class from below, say by \( \frac{2}{\Lambda} \), we can control its VC-dimension. Support Vector Machines, which we shall treat more closely in Section IV-A, implement this insight. The choice of linear functions seems to be very limiting (i.e. instead of being likely to overfit we are now more likely to underfit). Fortunately there is a way to have both, linear models and

There are some ramifications to this statement, that go beyond the scope of this work. Strictly speaking, VC theory requires the structure to be defined a priori, which has implications for the definition of the class of separating hyperplanes, cf. [47].

Fig. 3. Linear classifier and margins: A linear classifier is defined by a hyperplane’s normal vector \( w \) and an offset \( b \), i.e. the decision boundary is \( \{x| \langle w, x \rangle + b = 0 \} \) (thick line). Each of the two halfspaces defined by this hyperplane corresponds to one class, i.e. \( f(x) = \text{sign}(\langle w, x \rangle + b) \). The margin of a linear classifier is the minimal distance of any training point to the hyperplane. In this case it is the distance between the dotted lines and the thick line.

or regression in \( \mathcal{F} \) is to be found. This is also implicitly done for (one hidden layer) neural networks, radial basis networks (e.g. [49], [50], [51], [52]) or Boosting algorithms [53] where the input data is mapped to some representation given by the hidden layer, the RBF bumps or the hypothesis space respectively.

The so-called \textit{curse of dimensionality} from statistics says essentially that the difficulty of an estimation problem increases drastically with the dimension \( N \) of the space, since – in principle – as a function of \( N \) one needs exponentially

a very rich set of nonlinear decision functions, by using the tools that will be discussed in the next section.

III. NONLINEAR ALGORITHMS IN KERNEL FEATURE SPACES

Algorithms in feature spaces make use of the following idea: via a nonlinear mapping

\[ \Phi : \mathbb{R}^N \rightarrow \mathcal{F} \]

\[ x \mapsto \Phi(x) \]

the data \( x_1, \ldots, x_n \in \mathbb{R}^N \) is mapped into a potentially much higher dimensional feature space \( \mathcal{F} \). For a given learning problem one now considers the same algorithm in \( \mathcal{F} \) instead of \( \mathbb{R}^N \), i.e. one works with the sample

\[ (\Phi(x_1), y_1), \ldots, (\Phi(x_n), y_n) \in \mathcal{F} \times \mathbb{Y}. \]

Given this mapped representation a \textit{simple} classification

or regression in \( \mathcal{F} \) is to be found. This is also implicitly done for (one hidden layer) neural networks, radial basis networks (e.g. [49], [50], [51], [52]) or Boosting algorithms [53] where the input data is mapped to some representation given by the hidden layer, the RBF bumps or the hypothesis space respectively.
many patterns to sample the space properly. This well known statement induces some doubts about whether it is a good idea to go to a high dimensional feature space for learning.

However, statistical learning theory tells us that the contrary can be true: learning in $\mathcal{F}$ can be simpler if one uses a low complexity, i.e. simple class of decision rules (e.g. linear classifiers). All the variability and richness that one needs to have a powerful function class is then introduced by the mapping $\Phi$. In short: not the dimensionality but the complexity of the function class matters [3]. Intuitively, this idea can be understood from the toy example in Figure 4: in two dimensions a rather complicated non-linear decision surface is necessary to separate the classes, whereas in a feature space of second order monomials (see e.g. [54])

$$\Phi: \mathbb{R}^2 \to \mathbb{R}^2$$

$$(x_1, x_2) \mapsto (z_1, z_2) := (x_1^2, \sqrt{2} x_1 x_2, x_2^2) \quad (6)$$

all one needs for separation is a linear hyperplane. In this simple toy example, we can easily control both: the statistical complexity (by using a simple linear hyperplane classifier) and the algorithmic complexity of the learning machine, as the feature space is only three dimensional. However, it becomes rather tricky to control the latter for large real world problems. For instance, consider images of $16 \times 16$ pixels as patterns and 5th order monomials as mapping $\Phi$ — then one would map to a space that contains all 5th order products of 256 pixels, i.e. to a $\left( \frac{5 + 256 - 1}{5} \right) \approx 10^{16}$-dimensional space. So, even if one could control the statistical complexity of this function class, one would still run into intractability problems while executing an algorithm in this space.

Fortunately, for certain feature spaces $\mathcal{F}$ and corresponding mappings $\Phi$ there is a highly effective trick for computing scalar products in feature spaces using kernel functions [55], [56], [1], [3]. Let us come back to the example from Eq. (6). Here, the computation of a scalar product between two feature space vectors, can be readily reformulated in terms of a kernel function $k$

$$(\Phi(x) \cdot \Phi(y)) = (x_1, \sqrt{2} x_1 x_2, x_2^2)(y_1, \sqrt{2} y_1 y_2, y_2^2)^T$$

$$= ((x_1, x_2)(y_1, y_2))^T$$

$$= (x \cdot y)^2$$

$$= k(x, y).$$

This finding generalizes:

- For $x, y \in \mathbb{R}^N$, and $d \in \mathbb{N}$ the kernel function

$$k(x, y) = (x \cdot y)^d$$

computes a scalar product in the space of all products of $d$ vector entries (monomials) of $x$ and $y$ [3], [11].

- If $k: \mathcal{C} \times \mathcal{C} \to \mathbb{R}$ is a continuous kernel of a positive integral operator on a Hilbert space $L_2(\mathcal{C})$ on a compact set $\mathcal{C} \subset \mathbb{R}^N$, i.e.

$$\forall f \in L_2(\mathcal{C}): \int_{\mathcal{C}} k(x, y) f(x) f(y) dx dy \geq 0,$$

then there exists a space $\mathcal{F}$ and a mapping $\Phi: \mathbb{R}^N \to \mathcal{F}$ such that $k(x, y) = (\Phi(x) \cdot \Phi(y))$ [3]. This can be seen directly from Mercer’s Theorem [39] saying that any kernel of a positive integral operator can be expanded in its eigenfunctions $\psi_j$ ($\lambda_j > 0, N_{\mathcal{F}} \leq \infty$):

$$k(x, y) = \sum_{j=1}^{N_{\mathcal{F}}} \lambda_j \psi_j(x) \psi_j(y).$$

In this case

$$\Phi(x) = (\sqrt{\lambda_1} \psi_1(x), \sqrt{\lambda_2} \psi_2(x), \ldots)$$

is a possible realization.

- Note furthermore that using a particular SV kernel corresponds to an implicit choice of a regularization operator (cf. [39], [57]). For translation invariant kernels, the regularization properties can be expressed conveniently in Fourier space in terms of the frequencies [58], [60]. For example Gaussian kernels (7) correspond to a general smoothness assumption in all $k$-th order derivatives [58]. Vice versa, using this correspondence, kernels matching a certain prior about the frequency content of the data can be constructed that reflect our prior problem knowledge.

Table II lists some of the most widely used kernel functions. More sophisticated kernels (e.g. kernels generating splines or Fourier expansions) can be found in [4], [36], [5], [58], [30], [28], [61].

A. Wrapping up

The interesting point about kernel functions is that the scalar product can be implicitly computed in $\mathcal{F}$, without explicitly using or even knowing the mapping $\Phi$. So, kernels allow to compute scalar products in spaces, where one could otherwise hardly perform any computations. A direct consequence from this finding is [11]: every (linear)

**Table II**

| Common kernel functions: Gaussian RBF ($c \in \mathbb{R}$), polynomial ($d \in \mathbb{N}, \theta \in \mathbb{R}$), sigmoidal ($c, \theta \in \mathbb{R}$) and inverse multiquadric ($c \in \mathbb{R}^+$) kernel functions are among the most common ones. While RBF and polynomial are known to fulfill Mercer’s condition, this is not strictly the case for sigmoidal kernels [33]. Further valid kernels proposed in the context of regularization networks are e.g. multiquadric or spline kernels [39], [57], [58]. |

<table>
<thead>
<tr>
<th>Kernel Type</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian RBF</td>
<td>$k(x, y) = \exp\left(-\frac{|x - y|^2}{c}\right)$</td>
</tr>
<tr>
<td>Polynomial</td>
<td>$(x \cdot y + \theta)^d$</td>
</tr>
<tr>
<td>Sigmoidal</td>
<td>$\tanh(\kappa(x \cdot y + \theta)$</td>
</tr>
<tr>
<td>Inv. multiquadric</td>
<td>$\frac{1}{\sqrt{|x - y|^2 + c^2}}$</td>
</tr>
</tbody>
</table>
algorithm that only uses scalar products can implicitly be executed in $\mathcal{F}$ by using kernels, i.e. one can very elegantly construct a nonlinear version of a linear algorithm.\footnote{Even algorithms that operate on similarity measures $k$ generating positive matrices $k(x_i, x_j)$ can be interpreted as linear algorithms in some feature space $\mathcal{F}$ [4].}

In the following sections we follow this philosophy for supervised and unsupervised learning: by (re-)formulating linear, scalar product based algorithms that are simple in feature space, one is able to generate powerful nonlinear algorithms, which use rich function classes in input space.

IV. Supervised Learning

We will now briefly outline the algorithms of SVMs and the Kernel Fisher Discriminant (KFD). Furthermore we discuss the Boosting algorithm from the kernel feature space point of view and show a connection to SVMs. Finally, we will point out some extensions of these algorithms proposed recently.

A. Support Vector Machines

Let us recall from Section II that the VC dimension of a linear system, e.g. separating hyperplanes (as computed by a perceptron)

$$y = \text{sign}((\mathbf{w} \cdot \mathbf{x}) + b)$$

can be upper bounded in terms of the margin (cf. (5)). For separating hyperplane classifiers the conditions for classification without training error are

$$y_i((\mathbf{w} \cdot \mathbf{x}_i) + b) \geq 1, \quad i = 1, \ldots, n.$$  \hspace{1cm} (8)

As linear function classes are often not rich enough in practice, we will follow the line of thought of the last section and consider linear classifiers in feature space using dot products. To this end, we substitute $\Phi(\mathbf{x}_i)$ for each training example $\mathbf{x}_i$, i.e. $y = \text{sign}((\mathbf{w} \cdot \Phi(\mathbf{x})) + b)$. In feature space, the conditions for perfect classification are described as

$$y_i((\mathbf{w} \cdot \Phi(\mathbf{x}_i)) + b) \geq 1, \quad i = 1, \ldots, n.$$  \hspace{1cm} (8)

The goal of learning is to find $\mathbf{w} \in \mathcal{F}$ and $b$ such that the expected risk is minimized. However, since we cannot obtain the expected risk itself, we will minimize the bound (3), which consists of the empirical risk and the complexity term. One strategy is to keep the empirical risk zero by constraining $\mathbf{w}$ and $b$ to the perfect separation case, while minimizing the complexity term, which is a monotonically increasing function of the VC dimension $h$. For a linear classifier in feature space the VC dimension $h$ is bounded according to $h \leq ||\mathbf{w}||^2 R^2 + 1$ (cf. (5)), where $R$ is the radius of the smallest ball around the training data (e.g. [3]), which is fixed for a given data set. Thus, we can minimize the complexity term by minimizing $||\mathbf{w}||^2$. This can be formulated as a quadratic optimization problem

$$\min_{\mathbf{w}, b} \frac{1}{2}||\mathbf{w}||^2$$  \hspace{1cm} (9)

subject to (8). However, if the only possibility to access the feature space is via dot-products computed by the kernel, we can not solve (9) directly since $\mathbf{w}$ lies in that feature space. But it turns out that we can get rid of the explicit usage of $\mathbf{w}$ by forming the dual optimization problem. Introducing Lagrange multipliers $\alpha_i \geq 0, \ i = 1, \ldots, n$, one for each of the constraints in (8), we get the following Lagrangian:

$$L(\mathbf{w}, b, \alpha) = \frac{1}{2}||\mathbf{w}||^2 - \sum_{i=1}^{n} \alpha_i (y_i((\mathbf{w} \cdot \Phi(\mathbf{x}_i)) + b) - 1).$$  \hspace{1cm} (10)

The task is to minimize (10) with respect to $\mathbf{w}$ and $b$ and to maximize it with respect to $\alpha_i$. At the optimal point, we have the following saddle point equations:

$$\frac{\partial L}{\partial b} = 0 \quad \text{and} \quad \frac{\partial L}{\partial \mathbf{w}} = 0,$$

which translate into

$$\sum_{i=1}^{n} \alpha_i y_i = 0 \quad \text{and} \quad \mathbf{w} = \sum_{i=1}^{n} \alpha_i y_i \Phi(\mathbf{x}_i).$$  \hspace{1cm} (11)

From the right equation of (11), we find that $\mathbf{w}$ is contained in the subspace spanned by the $\Phi(\mathbf{x}_i)$. By substituting (11) into (10) and by replacing $(\Phi(\mathbf{x}_i) \cdot \Phi(\mathbf{x}_j))$ with kernel functions $k(x_i, x_j)$, we get the dual quadratic optimization problem:

$$\max_{\alpha} \quad \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j k(x_i, x_j)$$

subject to $\alpha_i \geq 0, \ i = 1, \ldots, n,$

$$\sum_{i=1}^{n} \alpha_i y_i = 0.$$  \hspace{1cm} (11)

Thus, by solving the dual optimization problem, one obtains the coefficients $\alpha_i, i = 1, \ldots, n$, which one needs to express the $\mathbf{w}$ which solves (9). This leads to the nonlinear decision function

$$f(\mathbf{x}) = \text{sgn} \left( \sum_{i=1}^{n} y_i \alpha_i (\Phi(\mathbf{x}) \cdot \Phi(\mathbf{x}_i)) + b \right)$$

$$= \text{sgn} \left( \sum_{i=1}^{n} y_i \alpha_i k(\mathbf{x}, \mathbf{x}_i) + b \right).$$

Note that we have up to now only considered the separable case. This corresponds to an empirical error of zero (cf. Theorem 1). However for noisy data, this might not be the minimum in the expected risk (cf. (3)) and we might face overfitting effects (cf. Fig. 1). Therefore a "good" trade-off between the empirical risk and the complexity term in (3) needs to be found. Using a technique which was first proposed in [62] and later used for SVMs in [2], one introduces slack-variables to relax the hard-margin constraints:

$$y_i((\mathbf{w} \cdot \Phi(\mathbf{x}_i)) + b) \geq 1 - \xi_i, \quad \xi_i \geq 0, \quad i = 1, \ldots, n.$$  \hspace{1cm} (12)
additionally allowing for some classification errors. The SVM solution can then be found by (a) keeping the upper bound on the VC dimension small and (b) by minimizing an upper bound \( \sum_{i=1}^{n} \xi_i \) on the empirical risk,\(^4\) i.e., the number of training errors. Thus, one minimizes

\[
\min_{w, b, \xi} \quad \frac{1}{2} ||w||^2 + C \sum_{i=1}^{n} \xi_i
\]

where the regularization constant \( C > 0 \) determines the trade-off between the empirical error and the complexity term. This leads to the dual problem:

\[
\max_{\alpha} \quad \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j k(x_i, x_j) \tag{13}
\]

subject to \( 0 \leq \alpha_i \leq C, \quad i = 1, \ldots, n, \) \( \sum_{i=1}^{n} \alpha_i y_i = 0. \) \( \tag{14} \)

From introducing the slack-variables \( \xi_i \), one gets the box constraints that limit the size of the Lagrange multipliers: \( \alpha_i \leq C, \quad i = 1, \ldots, n. \)

A.1 Sparsity

Most optimization methods are based on the second order optimality conditions, so called Karush-Kuhn-Tucker conditions which state necessary and in some cases sufficient conditions for a set of variables to be optimal for an optimization problem. It comes handy that these conditions are particularly simple for the dual SVM problem (13) [64]:

\[
\alpha_i = 0 \quad \Rightarrow \quad y_i f(x_i) \geq 1 \quad \text{and} \quad \xi_i = 0
\]

\[
0 < \alpha_i < C \quad \Rightarrow \quad y_i f(x_i) = 1 \quad \text{and} \quad \xi_i = 0
\]

\[
\alpha_i = C \quad \Rightarrow \quad y_i f(x_i) \leq 1 \quad \text{and} \quad \xi_i \geq 0
\]

They reveal one of the most important property of SVMs: the solution is sparse in \( \alpha \), i.e., many patterns are outside the margin area and the optimal \( \alpha_i \)'s are zero. Specifically, the KKT conditions show that only such \( \alpha_i \) connected to a training pattern \( x_i \), which is either on the margin (i.e., \( 0 < \alpha_i < C \)) or inside the margin area (i.e., \( \alpha_i = C \)) and \( y_i f(x_i) < 1 \) are non-zero. Without this sparsity property, SVM learning would hardly be practical for large data sets.

A.2 \( \nu \)-SVMs

Several modifications have been proposed to the basic SVM algorithm. One particular useful modification are \( \nu \)-SVMs [65], originally proposed for regression. In the case of pattern recognition, they replace the rather un-intuitive regularization constant \( C \) with another constant \( \nu \in (0, 1] \) and yield, for appropriate parameter choices, identical solutions. Instead of (13) one solves

\[
\max_{\alpha} \quad \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j k(x_i, x_j) \cdot \nu
\]

subject to \( 0 \leq \alpha_i \leq 1/n, \quad i = 1, \ldots, n, \)

\[
\sum_{i=1}^{n} \alpha_i y_i = 0, \quad \sum \alpha_i \geq \nu.
\]

The advantage is that this new parameter \( \nu \) has a clearer interpretation than simply “the smaller, the smoother”: under some mild assumptions (data i.i.d. from continuous probability distribution [65]) it is asymptotically (i) an upper bound on the number of margin errors\(^5\) and (ii) a lower bound on the number of support vectors.

A.3 Computing the Threshold

The threshold \( b \) can be computed by exploiting the fact that for all SVs \( x_i \) with 0 < \( \alpha_i < C \), the slack variable \( \xi_i \) is zero. This follows from the Karush-Kuhn-Tucker (KKT) conditions (cf. (16)). Thus, for any support vector \( x_i \) with \( i \in I := \{ i : 0 < \alpha_i < C \} \) holds:

\[
y_i \left(b + \sum_{j=1}^{n} y_j \alpha_j k(x_i, x_j)\right) = 1.
\]

Averaging over these patterns yields a numerically stable solution:

\[
b = \frac{1}{|I|} \sum_{i \in I} \left(y_i - \sum_{j=1}^{n} y_j \alpha_j k(x_i, x_j)\right).
\]

A.4 A geometrical explanation

Here, we will present an illustration of the SVM solution to enhance intuitive understandings. Let us normalize the weight vector to 1 (i.e., \( ||w||^2 = 1 \)) and fix the threshold \( b = 0 \). Then, the set of all \( w \) which separate the training samples is completely described as

\[
\mathcal{V} = \{ w | y_i f(x_i) > 0; \quad i = 1, \ldots, n; \quad ||w||^2 = 1 \}
\]

The set \( \mathcal{V} \) is called “version space” [66]. It can be shown that the SVM solution coincides with the Tchebycheff-center of the version space, which is the center of the largest sphere contained in \( \mathcal{V} \) (cf. [67]). However, the theoretical optimal point in version space yielding a Bayes-optimal decision boundary is the Bayes point, which is known to be closely approximated by the center of mass [68], [69]. The version space is illustrated as a region on the sphere as shown in Figures 5 and 6. If the version space is shaped as in Figure 5, the SVM solution is near to the optimal point. However, if it has an elongated shape as in Figure 6, the SVM solution is far from the optimal one. To cope with this problem, several researchers [70], [68], [71] proposed a billiard sampling method for approximating the Bayes point. This method can achieve improved results, as shown on several benchmarks in comparison to SVMs.

\(^4\)Other bounds on the empirical error, like \( \sum_{i=1}^{n} \xi_i^2 \) are also frequently used (e.g., [2], [63]).

\(^5\)A margin error is a point \( x_i \) which is either being misclassified or lying inside the margin area.
5. Optimization Techniques for SVMs

To solve the SVM problem one has to solve the (convex) quadratic programming (QP) problem (13) under the constraints (14) and (15) (Eq. (13) can be rewritten as maximizing $-\frac{1}{2} \alpha^T K \alpha + \mathbf{1}^T \alpha$ where $K$ is the positive semidefinite matrix $K_{ij} = y_i y_j k(x_i, x_j)$ and 1 the vector of all ones). As the objective function is convex every (local) maximum is already a global maximum. However, there can be several optimal solutions (in terms of the variables $\alpha_i$) which might lead to different testing performances.

There exists a huge body of literature on solving quadratic programs and several free or commercial software packages (see e.g. [73], [74], [33] and references therein). However, the problem is that most mathematical programming approaches are either only suitable for small problems or assume that the quadratic term covered by $K$ is very sparse, i.e. most elements of this matrix are zero. Unfortunately this is not true for the SVM problem and thus using standard codes with more than a few hundred variables results in enormous training times and more than demanding memory needs. Nevertheless, the structure of the SVM optimization problem allows to derive specially tailored algorithms which allow for fast convergence with small memory requirements even on large problems. Here we will briefly consider three different approaches. References, containing more details and tricks can be found e.g. in [6], [33].

A.5.a Chunking. A key observation in solving large scale SVM problems is the sparsity of the solution $\alpha$. Depending on the problem, many of the optimal $\alpha_i$ will either be zero or on the upper bound $C$. If one knew beforehand which $\alpha_i$ were zero, the corresponding rows and columns could be removed from the matrix $K$ without changing the value of the quadratic form. Further, a point $\alpha$ can only be optimal for (13) if and only if it fulfills the KKT conditions (cf. (16)). In [64] a method called chunking is described, making use of the sparsity and the KKT conditions. At every step chunking solves the problem containing all non-zero $\alpha_i$ plus some of the $\alpha_i$ violating the KKT conditions. The size of this problem varies but is finally equal to the number of non-zero coefficients. While this technique is suitable for fairly large problems it is still limited by the maximal number of support vectors that one can handle and it still requires a quadratic optimizer to solve the sequence of smaller problems. A free implementation can be found e.g. in [75].

A.5.b Decomposition Methods. Those methods are similar in spirit to chunking as they solve a sequence of small QPs as well. But here the size of the subproblems is fixed. They are based on the observations of [76], [77] that a sequence of QPs which at least always contains one sample violating the KKT conditions will eventually converge to the optimal solution. It was suggested to keep the size of the subproblems fixed and to add and remove one sample in each iteration. This allows the training of arbitrary large data sets. In practice, however, the convergence of such an approach is very slow. Practical implementations use sophisticated heuristics to select several patterns to add and remove from the subproblem plus efficient caching methods. They usually achieve fast convergence even on large datasets with up to several thousands of support vectors. A good quality (free) implementation is SVMlight [78]. A quadratic optimizer is still required and contained in the package. Alternatively, the package [75] also contains a decomposition variant.

A.5.c Sequential Minimal Optimization (SMO). This method proposed by [79] can be viewed as the most extreme case of decomposition methods. In each iteration it solves a quadratic problem of size two. This can be done analytically and thus no quadratic optimizer is required. Here the main problem is to chose a good pair of variables to optimize in each iteration. The original heuristics presented in [79] are based on the KKT conditions and there has been some work (e.g. [80]) to improve them. The implementation of the SMO approach is straightforward (pseudo code in [79]). While the original work was targeted at an SVM for classification, there are now also approaches which implement variants of SMO for SVM regression (e.g. [36], [33]) and single-class SVMs (cf. below, [14]).
A.5.4 Other techniques. Further algorithms have been proposed to solve the SVM problem or a close approximation. For instance, the Kernel-Adatron [81] is derived from the Adatron algorithm by [82] proposed originally in a statistical mechanics setting. It constructs a large margin hyperplane using online learning. Its implementation is very simple. However, its drawback is that it does not allow for training errors, i.e., it is only valid for separable data sets. In [83] a slightly more general approach for data mining problems is considered.

A.5.5 Codes. A fairly large selection of optimization codes for SVM classification and regression may be found on the web at [84] together with the appropriate references. They range from simple MATLAB implementation to sophisticated C, C++ or FORTRAN programs. Note that most of these implementations are for non-commercial use only.

B. Kernel Fisher Discriminant

The idea of the Kernel Fisher Discriminant (KFD) (e.g. [7], [9], [10]) is to solve the problem of Fisher’s linear discriminant [85], [86] in a kernel feature space \( \mathcal{F} \), thereby yielding a nonlinear discriminant in the input space. In the linear case, Fisher’s discriminant aims at finding a linear projections such that the classes are well separated (cf. Figure 7). Separability is measured by two quantities: How far are the projected means apart (should be large) and how big is the variance of the data in this direction (should be small). This can be achieved by maximizing the Rayleigh coefficient

\[
J(w) = \frac{w^T S_B w}{w^T S_W w},
\]

of between and within class variance with respect to \( w \), where

\[
S_B = (m_2 - m_1)(m_2 - m_1)^T
\]

and

\[
S_W = \sum_{k=1,2} \sum_{i \in I_k} (x_i - m_k)(x_i - m_k)^T.
\]

Here \( m_k \) and \( I_k \) denote the sample mean and the index set for class \( k \), respectively. Note, that under the assumption that the class distributions are (identically distributed) Gaussians, Fisher’s discriminant is Bayes optimal; it can also be generalized to the multi-class case. To formulate the problem in a kernel feature space \( \mathcal{F} \) one can make use of a similar expansion as (11) in SVMs for \( w \in \mathcal{F} \), i.e., one can express \( w \) in terms of mapped training patterns [7]:

\[
w = \sum_{i=1}^{n} \alpha_i \Phi(x_i).
\]

Substituting \( \Phi(x) \) for all \( x \) in (17) and plugging in (18), the optimization problem for the KFD in the feature space can then be written as [8]:

\[
J(\alpha) = \frac{\alpha^T \mu_k^2}{\alpha^T N \alpha} = \frac{\alpha^T M \alpha}{\alpha^T N \alpha},
\]

where \( \mu_k = \frac{1}{|I_k|} \sum_{x_i \in I_k} \Phi(x_i) \), \( N = \sum_{k=1,2} |I_k| \mu_k \mu_k^T \), \( \mu = \mu_2 - \mu_1 \), \( M = \mu \mu^T \), and \( K_{ij} = \Phi(x_i) \cdot \Phi(x_j) \) = \( k(x_i, x_j) \).

The projection of a test point onto the discriminant is computed by

\[
(w \cdot \Phi(x)) = \sum_{i=1}^{n} \alpha_i k(x_i, x).
\]

Finally, to use this projections in classification one needs to find a suitable threshold which can either be chosen as the mean of the average projections of the two classes or, e.g., by training a linear SVM on the projections.

As outlined before, the dimension of the feature space is equal to or higher than the number of training samples \( n \) which makes regularization necessary. In [7] it was proposed to add a multiple of e.g. the identity or the kernel matrix \( N \) to \( P \), penalizing \( \|\alpha\|^2 \) or \( |w|^2 \), respectively (see also [87], [88]).

To maximize (19) one could either solve the generalized eigenproblem \( M \alpha = \lambda N \alpha \), selecting the Eigenvector \( \alpha \) with maximal Eigenvalue \( \lambda \), or, equivalently, compute \( \alpha \equiv N^{-1}(\mu_2 - \mu_1) \). However, as the matrices \( N \) and \( M \) scale with the number of training samples and the solutions are non-sparse this is only feasible for moderate \( n \).

One possible solution is to transform KFD into a convex quadratic programming problem [89] which allows to derive a sparse variant of KFD and a more efficient, sparse-greedy approximation algorithm [90]. Recalling that Fisher’s Discriminant tries to minimize the variance of the data along the projection whilst maximizing the distance between the average outputs for each class, the following quadratic program does exactly this:

\[
\min_{\alpha, \xi, \xi} \quad \|\xi\|^2 + C P(\alpha)
\]

subject to

\[
K \alpha + b = y + \xi,
\]

\[
1^T \xi = 0 \quad \text{for} \quad k = 1, 2,
\]

for \( \alpha, \xi \in \mathbb{R}^n \), and \( b, C \in \mathbb{R} \). Here P is a regularizer as mentioned before and (1_1_k) is one for \( y_k \) belonging to class \( k \) and zero otherwise. It is straightforward to show, that

\[\text{This can be done with kernel functions as well and has explicitly been carried out e.g. in [9], [10]. However, most further developments for KFD do not easily carry over to the multi-class case, e.g. resulting in integer programming problems.}\]
this program is equivalent to (19) with the same regularizer added to the matrix $N$ [89]. The proof is based on the facts
the (i) the matrix $M$ is rank one and (ii) that the solutions $w$ to (19) are invariant under scaling. Thus one can fix the
distance of the means to some arbitrary, positive value, say two, and just minimize the variance. The first constraint, which can be read as $(w \cdot x_i) + b = y_i + \xi_i, i = 1, \ldots, n$, pulls the output for each sample to its class-label. The term $\|\xi\|^2$
minimizes the variance of the error committed, while the constraints $\sum_i \xi_i = 0$ ensure that the average output for each
class is the label, i.e. for $\pm 1$ labels the average distance of the projections is two. For $C = 0$ one obtains the original
Fisher algorithm in feature space.

B.1 Optimization

Besides a more intuitive understanding of the mathematical properties of KFD [89], in particular in relation to
SVMs or the Relevance Vector Machine (RVM) [91], the formulation (20) allows to derive more efficient algorithms
as well. Choosing a $\ell_1$-norm regularizer $P(\alpha) = \|\alpha\|$, we obtain sparse solutions (sparse KFD (SKFD))
by going even further and replacing the quadratic penalty on the variables $\xi$ with an $\ell_1$-norm as well, we obtain a linear
program which can be very efficiently optimized using column generation techniques (e.g. [92]) (Linear Sparse
KFD (LSKFD)). An alternative optimization strategy arising from (20) is to iteratively construct a solution to the full
problem as proposed in [90]. Starting with an empty solution one adds in each iteration one pattern to the expansion
(18). This pattern is chosen such that it (approximately) gives the largest decrease in the objective function (other
criteria are possible). When the change in the objective falls below a predefined threshold the iteration is terminated.
The obtained solution is sparse and yields competitive results compared to the full solution. The advantages of this
approach are the smaller memory requirements and faster training time compared to quadratic programming
or the solution of an Eigenproblem.

C. Connection between Boosting and Kernel Methods

We will now show a connection of Boosting to SVMs and KFD. Let us start with a very brief review of Boosting
methods, which does not claim to be complete – for more details see e.g. [93], [33], [94], [95], [96], [97].

The first boosting algorithm was proposed by Rob Schapire [98]. This algorithm was able to "boost" the performance of a
weak PAC learner [99] such that the resulting algorithm satisfies the strong PAC learning criteria [100].

Freund and Schapire found an improved PAC boosting algorithm – called AdaBoost [53] – which repeatedly calls a
given "weak learner" (also known as base learning algorithm) $\mathcal{L}$ and finally produces a master hypothesis $f$ which is a convex
combination of the functions $h_j$ produced by the base learning
algorithm, i.e. $f(x) = \sum_{t=1}^T w_t h_t(x)$ and $w_t \geq 0, 
t = 1, \ldots, T$. The given weak learner $\mathcal{L}$ is used with different
parameters $p = [p_1, \ldots, p_n]$ (where $\sum_i p_i = 1, 
p_i \geq 0, i = 1, \ldots, n$) on the training set, which are chosen in such a way that patterns poorly classified by the
current master hypothesis are more emphasized than other patterns.

Recently, several researchers [101], [102], [103], [104] have noticed that AdaBoost implements a constraint gradient-descent
(coordinate-descent) method on an exponential function of the margins. From this understanding, it is apparent that other algorithms can be derived [101], [102], [103], [104].

A slight modification of AdaBoost – called Arc-Boost – has been proposed in [105]. For Arc-Boost it
is easy to prove that it asymptotically (with the number of iterations) finds a convex combination of all possible base
hypotheses that maximizes the margin – very much in spirit to the hard margin SVM mentioned in Section IV-A. Let $H := \{h_j \mid j = 1, \ldots, J\}$ be the set of hypotheses, from which the base learner can potentially select hypotheses.

Then the solution of Arc-Boost is the same as one of the following linear program [105], that maximizes the smallest margin $\rho$:

$$\max_{w \in \mathcal{F}, \rho \in \mathbb{R}^+} \rho$$

subject to

$$y_i \sum_{j=1}^J w_j h_j(x_i) \geq \rho \quad \text{for} \quad i = 1, \ldots, n$$

$$\|w\|_1 = 1.$$ (21)

Let us recall that SVMs and KFD implicitly compute scalar products in feature space with the help of the kernel
trick. Omitting the bias ($b \equiv 0$) for simplicity, the SVM
minimization of (9) subject to (8) can be restated as a maximization of the margin $\rho$ (cf. Fig. 3)

$$\max_{w \in \mathcal{F}, \rho \in \mathbb{R}^+} \rho$$

subject to

$$y_i \sum_{j=1}^N w_j P_j[\Phi(x_i)] \geq \rho \quad \text{for} \quad i = 1, \ldots, n$$

$$\|w\|_2 = 1,$$ (22)

where $N = \dim(\mathcal{F})$ and $P_j$ is the operator projecting onto the $j$-th coordinate in feature space. The use of the $\ell_2$-
norm of $w$ in the last constraint implies that the resulting
hyperplane is chosen such that the minimum $\ell_2$-distance of a training pattern to the hyperplane is maximized (cf. Section
II-B). More generally, using an arbitrary $\ell_p$-norm

[\textit{Footnotes:}]

1 Roughly speaking, a reason for the induced sparseness is the fact that vectors far from the coordinate axes are "larger" with respect to the $\ell_1$-norm than with respect to $\ell_p$-norms with $p > 1$.

2 For example, consider the vectors $(1, 0)$ and $(1/\sqrt{2}, 1/\sqrt{2})$. For the two norms, $\|(1, 0)\|_2 = \|1/\sqrt{2}, 1/\sqrt{2}\|_2 = 1$, but for the $\ell_1$-norm, $1 = \|(1, 0)\|_1 < \|1/\sqrt{2}, 1/\sqrt{2}\|_1 = \sqrt{2}$. Note that using the $\ell_1$-
norm as regularizer the optimal solution is always a vertex solution (or can be expressed as such) and tends to be very sparse.

3 A method that builds a strong PAC learning algorithm from a weak PAC learning algorithm is called a PAC boosting algorithm

[96].

9 cf. also [96] for an investigation in which potentials lead to PAC
boosting algorithms.

10 A generalization of Arc-Boost using slack variables as in Eq. (12) can be found in [106], [92].
constraint on the weight vector leads to maximizing the \(\ell_\infty\)-distance between hyperplane and training points \([107]\), where \(\frac{1}{q} + \frac{1}{p} = 1\). Thus, in (21) one maximizes the minimum \(\ell_\infty\)-distance of the training points to the hyperplane.

On the level of the mathematical programs (22) and (21), one can clearly see the relation between Boosting and SVMs. The connection can be made even more explicit by observing that any hypothesis set \(H\) implies a mapping \(\Phi\) by

\[
\Phi : \mathbf{x} \mapsto [h_1(\mathbf{x}), \ldots, h_N(\mathbf{x})]^T,
\]

and therefore also a kernel \(k(\mathbf{x}, \mathbf{y}) = (\Phi(\mathbf{y}) \cdot \Phi(\mathbf{y})) = \sum_{j=1}^{N} h_j(\mathbf{x})h_j(\mathbf{y}),\) which could in principle be used for SVM learning. Thus, any hypothesis set \(H\) spans a feature space \(\mathcal{F}\). Furthermore, for any feature space \(\mathcal{F}\) which is spanned by some mapping \(\Phi\), the corresponding hypothesis set \(H\) can be readily constructed by \(h_j = P_j[\Phi]\).

Boosting, in contrast to SVMs, performs the computation explicitly in feature space. This is well-known to be prohibitive, if the solution \(\mathbf{w}\) is not sparse, as the feature space might be very high dimensional. As mentioned in Section IV-B (cf. Footnote 7), using the \(\ell_1\)-norm instead of the \(\ell_2\)-norm, one can expect to get sparse solutions in \(\mathbf{w}\), \(^{11}\) This might be seen as one important ingredient for Boosting, as it relies on the fact that there are only a few hypotheses/dimensions \(h_j = P_j[\Phi]\) needed to express the solution, which Boosting tries to find during each iteration. Basically, Boosting considers only the most important dimensions in feature space and can this way be very efficient.

D. Wrapping Up

SVMs, KFD and Boosting work in very high-dimensional feature spaces. They differ, however, in how they deal with the algorithmic problems that this can cause. One can think of boosting as an SV approach in a high dimensional feature space spanned by the base hypothesis of some function set \(H\). The problem becomes tractable since Boosting uses effectively a \(\ell_1\)-norm regularizer. This induces sparsity, hence one never really works in the full space, but always in a small subspace. Vice versa, one can think of SVMs and KFD as a “boosting approach” in a high-dimensional space. There we use the kernel trick and therefore never explicitly work in the feature space. Thus, SVMs and KFD get away without having to use \(\ell_1\)-norm regularizers; indeed, they could not use them on \(\mathbf{w}\), as the kernel only allows computation of the \(\ell_2\)-norm in feature space. SVM and Boosting lead to sparse solutions (as does KFD with the appropriate regularizer \([89]\)), although in different spaces, and both algorithms are constructed to exploit the form of sparsity they produce. Besides providing insight, this correspondence has concrete practical benefits for designing new algorithms. Almost any new development in the field of SVMs can be translated to a corresponding Boosting algorithm using the \(\ell_1\)-norm instead of the \(\ell_2\)-norm and vice versa (cf. \([106],[109],[110]\)).

\(^{11}\)Note that the solution of SVMs is under rather mild assumption not sparse in \(\mathbf{w} = \sum_{i=1}^{\infty} \alpha_i \Phi(\mathbf{x}_i)\) \([108]\), but in \(\alpha\).

V. UNSUPERVISED LEARNING

In unsupervised learning only the data \(\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{R}^N\), is given, i.e. the labels are missing. Standard questions of unsupervised learning are clustering, density estimation, and data description (see e.g. \([111],[51]\)). As already outlined above, the kernel trick cannot only be applied in supervised learning scenarios, but also for unsupervised learning, given that the base algorithm can be written in terms of scalar products. In the following sections we will first review one of the most common statistical data analysis algorithm, PCA, and explain its “kernelized” variant: kernel PCA (see \([11]\)). Subsequently, single-class classification is explained. Here the support of a given data set is being estimated (see e.g. \([14],[112],[113],[110]\)). Recently, single-class SVMs are frequently used in outlier or novelty detection applications.

A. Kernel PCA

The basic idea of PCA is depicted in Figure 8. For \(N\)-dimensional data, a set of orthogonal directions—capturing most of the variance in the data—is computed, i.e. the first \(k\) projections \((k = 1, \ldots, N)\) allow to reconstruct the data with minimal quadratic error. In practice one typically wants to describe the data with reduced dimensionality by extracting a few meaningful components, while at the same time one is retaining most existing structure in the data (see e.g. \([114]\)). Since PCA is a linear algorithm it is clearly beyond its capabilities to extract nonlinear structures in the data as, e.g., the one observed in Figure 8. It is here, where the Kernel-PCA algorithm sets in. To derive Kernel-PCA we first map the data \(\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{R}^N\) into a feature space \(\Phi(\mathbf{x})\).

![Fig. 8. By using a kernel function, Kernel-PCA is implicitly performing a linear PCA in some high dimensional feature space, that is nonlinearly related to input space. Linear PCA in the input space (top) is not sufficient to describe the most interesting direction in this toy example. Contrary, using a suitable nonlinear mapping \(\Phi\) and performing linear PCA on the mapped patterns (Kernel PCA), the resulting nonlinear direction in the input space can find the most interesting direction (bottom) (figure from \([11]\)).](image-url)
space $\mathcal{F}$ (cf. Section III) and compute the covariance matrix

$$ C = \frac{1}{n} \sum_{j=1}^{n} \Phi(x_j)\Phi(x_j)^\top. $$

The principal components are then computed by solving the Eigenvalue problem: find $\lambda > 0, \mathbf{V} \neq 0$ with

$$ \lambda \mathbf{V} = C \mathbf{V} = \frac{1}{n} \sum_{j=1}^{n} (\Phi(x_j) \cdot \mathbf{V})\Phi(x_j). \quad (23) $$

Furthermore, as can be seen from (23) all Eigenvectors with non-zero Eigenvalue must be in the span of the mapped data, i.e. $\mathbf{V} \in \text{span}\{\Phi(x_1), \ldots, \Phi(x_n)\}$. This can be written as

$$ \mathbf{V} = \sum_{i=1}^{n} \alpha_i \Phi(x_i). $$

By multiplying with $\Phi(x_k)$ from the left (23) reads

$$ \lambda(\Phi(x_k) \cdot \mathbf{V}) = (\Phi(x_k) \cdot C \mathbf{V}) \text{ for all } k = 1, \ldots, n. $$

Defining an $n \times n$-matrix

$$ K_{ij} := (\Phi(x_i) \cdot \Phi(x_j)) = k(x_i, x_j) \quad (24) $$

one computes an Eigenvalue problem for the expansion coefficients $\alpha_i$, that is now solely dependent on the kernel function

$$ \lambda \alpha = K \alpha \quad (\alpha = (\alpha_1, \ldots, \alpha_n)^\top). $$

The solutions $(\lambda_k, \alpha^k)$ further need to be normalized by imposing $\lambda_k (\alpha^k \cdot \alpha^k) = 1$ in $\mathcal{F}$. Also as in every PCA algorithm the data needs to be centered in $\mathcal{F}$. This can be done by simply substituting the kernel-matrix $K$ with

$$ \tilde{K} = K - 1_n K - K 1_n + 1_n K 1_n, $$

where $(1_n)_ij = 1/n$; for details see [11].

For extracting features of a new pattern $x$ with kernel PCA one simply projects the mapped pattern $\Phi(x)$ onto $\mathbf{V}^k$

$$ (\mathbf{V}^k \cdot \Phi(x)) = \sum_{i=1}^{M} \alpha^k_i (\Phi(x_i) \cdot \Phi(x)) = \sum_{i=1}^{M} \alpha^k_i k(x_i, x). \quad (25) $$

Note that in this algorithm for nonlinear PCA the nonlinearity enters the computation only at two points that do not change the nature of the algorithm: (a) in the calculation of the matrix elements of $K$ (24), and (b) in the evaluation of the expansion (25). So, for obtaining the Kernel-PCA components one only needs to solve a similar linear Eigenvalue problem as before for linear PCA, the only difference being that one has to deal with an $n \times n$ problem instead of an $N \times N$ problem. Clearly, the size of this problem becomes problematic for large $n$. [115] proposes to solve this by using a sparse approximation of the matrix $K$ which still describes the leading Eigenvectors sufficiently well. In [116] a sparse kernel PCA approach is proposed, set within a Bayesian framework. Finally, the approach given in [117] places a $\ell_1$-regularizer into the (kernel) PCA problem with the effect of obtaining sparse solutions as well as a comparably low computational cost. Figures 9 – 11 show examples for feature extraction with linear PCA and Kernel-PCA for artificial data sets. Further applications of kernel PCA for real world data can be found in Section VII-A.1 for OCR or in Section VII-C.1 for denoising problems, other applications are found in e.g. [6], [12], [119].

B. Single-Class Classification

A classical unsupervised learning task is density estimation. Assuming that the unlabeled observations $x_1, \ldots, x_n$ were generated i.i.d. according to some unknown distribution $P(x)$, the task is to estimate its density. However, there are several difficulties to this task. First, a density need not always exist — there are distributions that do not possess a density. Second, estimating densities exactly is
known to be a hard task. In many applications it is enough to estimate the support of a data distribution instead of the full density. Single-class SVMs avoid solving the harder density estimation problem and concentrate on the simpler task [3], i.e. estimating quantiles of the multivariate distribution, i.e. its support. So far there are two independent algorithms to solve the problem in a kernel feature space. They differ slightly in spirit and geometric notion [113], [14]. It is, however, not quite clear which of them is to be preferred in practice (cf. Figures 12 and 13). One solution of the single-class SVM problem by Tax and Duin [113] uses spheres with soft margins to describe the training data, close in spirit to the algorithm of [120]. For certain classes of kernels, such as Gaussian RBF ones, this sphere single-class SVM algorithm can be shown to be equivalent to the second Ansatz which is due to Schölkopf et al. [14].

For brevity we will focus on this second approach as it is more in the line of this review since it uses margin arguments. It computes a hyperplane in feature space such that a pre-specified fraction of the training example will lie beyond that hyperplane, while at the same time the hyperplane has maximal distance (margin) to the origin. For an illustration see Figure 12. To this end, we solve the following quadratic program [14]:

\[
\begin{align*}
\min_{w \in F, \xi \in \mathbb{R}^n, \rho \in \mathbb{R}} & \quad \frac{1}{2}||w||^2 + \frac{1}{m} \sum \xi_i - \rho \\
\text{subject to} & \quad (w \cdot \Phi(x_i)) \geq \rho - \xi_i, \quad \xi_i \geq 0.
\end{align*}
\]

Here, \( \nu \in (0,1] \) is a parameter akin to the one described above for the case of pattern recognition. Since nonzero slack variables \( \xi_i \) are penalized in the objective function, we can expect that if \( w \) and \( \rho \) solve this problem, then the decision function \( f(x) = \text{sign}(w \cdot \Phi(x) - \rho) \) will be positive for most examples \( x_i \) contained in the training set, while the SV type regularization term \( ||w|| \) will still be small. The actual trade-off between these two goals is controlled by \( \nu \). Deriving the dual problem, the solution can be shown to have a SV expansion (again, patterns \( x_i \) with nonzero \( \alpha_i \) are called SVs)

\[
f(x) = \text{sign} \left( \sum_i \alpha_i k(x_i, x) - \rho \right),
\]

where the coefficients are found as the solution of the dual problem:

\[
\begin{align*}
\min_{\alpha} & \quad \frac{1}{2} \sum_{ij} \alpha_i \alpha_j k(x_i, x_j) \\
\text{subject to} & \quad 0 \leq \alpha_i \leq 1/(mn), i = 1, \ldots, n \\
& \quad \sum_{i=1}^n \alpha_i = 1.
\end{align*}
\]

This problem can be solved with standard QP routines. It does, however, possess features that sets it apart from generic QPs, most notably the simplicity of the constraints. This can be exploited by applying a variant of SMO developed for this purpose [14].

The offset \( \rho \) can be recovered by exploiting that for any \( \alpha_i \) which is not at the upper or lower bound, the corresponding pattern \( x_i \) satisfies \( \rho = (w \cdot \Phi(x_i)) = \sum_j \alpha_j k(x_j, x_i) \).

Note that if \( \nu \) approaches 0, the upper boundaries on the Lagrange multipliers tend to infinity, i.e. the first inequality constraint in (28) becomes void. The problem then resembles the corresponding hard margin algorithm, since the penalization of errors becomes infinite, as can be seen from the primal objective function (26). It can be shown that if the data set is separable from the origin, then this
algorithm will find the unique supporting hyperplane with the properties that it separates all data from the origin, and its distance to the origin is maximal among all such hyperplanes. If, on the other hand, \( \nu \) equals 1, then the constraints alone only allow one solution: the one where all \( \alpha_i \) are at the upper bound \( 1/(nm) \). In this case, for kernels with integral 1, such as normalized versions of (7), the decision function corresponds to a thresholded Parzen windows estimator. For the parameter \( \nu \) one can show that it controls the fraction of errors and SVs (along the lines of Section IV-A).

**Theorem 2** ([14]) Assume the solution of (27) satisfies \( \rho \neq 0 \). The following statements hold:

(i) \( \nu \) is an upper bound on the fraction of outliers.

(ii) \( \nu \) is a lower bound on the fraction of SVs.

(iii) Suppose the data were generated independently from a distribution \( P(x) \) which does not contain discrete components. Suppose, moreover, that the kernel is analytic and non-constant. When the number \( n \) of samples goes to infinity, with probability 1, \( \nu \) equals both the fraction of SVs and the fraction of outliers.

We have thus described an algorithm which will compute a region that captures a certain fraction of the training examples. It is a “nice” region, as it will correspond to a small value of \( ||w||^2 \), thus the underlying function will be smooth [38]. How about test examples? Will they also lie inside the computed region? This question is the subject of single-class generalization error bounds [14]. Roughly, they state the following: suppose the estimated hyperplane has a small \( ||w||^2 \) and separates part of the training set from the origin by a certain margin \( \rho / ||w|| \). Then the probability that test examples coming from the same distribution lie outside of a slightly larger region will not be much larger than the fraction of training outliers.

Figure 14 displays 2-D toy examples, and shows how the parameter settings influence the solution. For further applications, including an outlier detection task in handwritten character recognition, cf. [14].

![Fig. 14. A single-class SVM using RBF kernel (7) applied to a toy problem: domain: [-1, 1]^2. First two pictures: Note how in both cases, at least a fraction of \( \nu \) of all examples is in the estimated region [cf. table]. The large value of \( \nu \) causes the additional data points in the upper left corner to have almost no influence on the decision function. For smaller values of \( \nu \), such as 0.1 (third picture), the points cannot be ignored anymore. Alternatively, one can force the algorithm to take these ‘outliers’ into account by changing the kernel width (7); in the fourth picture, using \( c = 0.1, \nu = 0.5 \), the data is effectively analyzed on a different length scale which leads the algorithm to consider the outliers as meaningful points. Figure taken from [14].](image)

<table>
<thead>
<tr>
<th>( \nu ), width ( c )</th>
<th>0.5, 0.5</th>
<th>0.5, 0.5</th>
<th>0.1, 0.5</th>
<th>0.5, 0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>frac. SVs/OEs</td>
<td>0.54, 0.43</td>
<td>0.39, 0.47</td>
<td>0.24, 0.03</td>
<td>0.65, 0.38</td>
</tr>
<tr>
<td>margin ( \rho /</td>
<td></td>
<td>w</td>
<td></td>
<td>)</td>
</tr>
</tbody>
</table>

**VI. Model Selection**

In the kernel methods discussed so far, the choice of the kernel has a crucial effect on the performance, i.e. if one does not choose the kernel properly, one will not achieve the excellent performance reported in many papers. **Model selection** techniques provide principled ways to select a proper kernel. Usually, the candidates of optimal kernels are prepared using some heuristic rules, and the one which minimizes a given criterion is chosen. There are three typical ways for model selection with different criteria, each of which is a prediction of the generalization error

(i) **Bayesian evidence framework** The training of a SVM is interpreted as Bayesian inference, and the model selection is done by maximizing the marginal likelihood (i.e. evidence), e.g. [121], [91].

(ii) **PAC** The generalization error is upper bounded using a capacity measure depending both on the weights and the model, and these are optimized to minimize the bound. The kernel selection methods for SVM following this approach are reported e.g. in [122], [36], [123].

(iii) **Cross validation** Here, the training samples are divided to \( k \) subsets, each of which have the same number of samples. Then, the classifier is trained \( k \)-times: In the \( i \)-th \((i = 1, \ldots, k) \) iteration, the classifier is trained on all subsets except the \( i \)-th one. Then the classification error is computed for the \( i \)-th subset. It is known that the average of these \( k \) errors is a rather good estimate of the generalization error [124]. The extreme case, where \( k \) is equal to the number of training samples, is called leave-one-out cross validation. Note that bootstrap [125], [126] is also a principled resampling method which is often used for model selection.

Other approaches, namely asymptotic statistical methods such as AIC [41] and NIC [43] can be used. However, since these methods need a large amount of samples by assumption, they have not been used in kernel methods so far. For (i) and (ii), the generalization error is approximated by expressions that can be computed efficiently. For small sample sizes, these values are sometimes not very accurate, but it is known that nevertheless often acceptable good models are selected. Among the three approaches, the most frequently used method is (iii) [124], but the problem is that the computational cost is the highest, because the learning problem must be solved \( k \) times. For SVM, there is an approximate way to evaluate the \( n \)-fold cross validation error (i.e. the leave-one-out classification error) called span bound [127]. If one assumes that the support vectors do not change even when a sample is left out, the leave-one-out classification result of this sample can be computed exactly. Under this assumption, we can obtain an estimate of the leave-one-out error – without retraining the SVM many times. Although this assumption is rather crude and not true in many cases, this approach gives a close approximation of the true leave-one-out error in experiments. For KFD there exists a similar result.

Now we would like to describe a particular efficient model selection method that has in practice often been used [128],
[102], [89], [7], [129], [130] in conjunction with the benchmark data sets described in Section VII-B.

In model selection for SVMs and KFD we have to determine the kernel parameters (one (RBF) or more (e.g., polynomial kernel)) and the regularization constant C or \( \nu \), while for Boosting one needs to choose the model parameters of the base learner, a regularization constant and the number of boosting iterations. Given a certain benchmark data set, one usually has a number, say \( M \) (e.g., 100), realizations, i.e., splits into training and test set, available (cf. Section VII-B). The different splits are often necessary to average the results in order to get more reliable estimates of the generalization error.

One possibility to do model selection would be to consider each realization independently from all others and to perform the cross-validation procedure \( M \) times. Then, for each realization one would end up with different model parameters, as the model selection on each realization will typically have various results.

It is less computationally expensive to have only one model for all realizations of one data set: To find this model, we run a 5-fold cross-validation procedure only on a few, say five, realizations of the data set. This is done in two stages: first a global search (i.e., over a wide range of the parameter space) is done to find a good guess of the parameter, which becomes more precise in the second stage. Finally, the model parameters are computed as the median of the five estimations and are used throughout the training on all \( M \) realization of the data set. This way of estimating the parameters is computationally still quite expensive, but much less expensive than the full cross validation approach mentioned above.

VII. Applications

This section describes selected\(^{12}\) interesting applications of supervised and unsupervised learning with kernels. It serves to demonstrate that kernel based approaches achieve competitive results over a whole range of benchmarks with different noise levels and robustness requirements.

A. Supervised Learning

A.1 OCR

Historically the first real-world experiments of SVMs\(^{13}\) – all done on OCR benchmarks (see Fig. 15) – exhibited quite high accuracies for SVMs [2], [120], [4], [131] comparably to state-of-the-art results achieved with convolutional multi-layer perceptrons [132], [133], [134], [135]. Table III shows the classification performance of SVMs in comparison to other state-of-the-art classifiers on the US-Postal Service (USPS) benchmark. Plain SVM give a performance very similar to other state-of-the-art methods. However SVMs can be strongly improved by using prior knowledge. For instance in [4] virtual support vectors have been generated by transforming the set of support vectors with an appropriate invariance transformation and retraining the machine on these vectors. Furthermore one can structure kernels such that they induce local invariances like translations, line thickening or rotations or that e.g., products of neighboring pixels in an image [131], that are thought to contain more information, are emphasized. So, prior knowledge can be used for engineering a larger data set or problem specific kernels (see also Section VII-A.2 for an application of this idea to DNA analysis). In a two stage process we also used kernel-PCA to extract features from the USPS data in the first step. A subsequent linear classification on these nonlinear features allowed to achieve an error rate of 4%, which is better by a factor of two than operating on linear PCA features (8.7%, cf. [11]).

A benchmark problem larger than the USPS data set (7291 patterns) was collected by NIST and contains 120000 handwritten digits. Invariant SVMs achieved the record error rate of 0.6% [18] on this challenging and more realistic data set, better than tangent distance (1.1%) and convolutional neural networks (LeNet 5: 0.9%). With an error rate of 0.7%, an ensemble of LeNet 4 networks that was trained on a vast number of artificially generated patterns (using invariance transformations) almost matches the performance of the best SVM [134].

A.2 Analyzing DNA Data

The genomic text contains untranslated regions and so called coding sequences (CDS) that encode proteins. In or-

\(^{12}\)Note that for our own convenience we have biased the selection towards applications pursued by the IDA group while adding abundant references to other work.

\(^{13}\)performed at AT&T Bell Labs.
order to extract protein sequences from nucleotide sequences, it is a central problem in computational biology to recognize the translation initiation sites (TIS) from which coding starts to determine which parts of a sequence will be translated and which not.

Coding sequences can in principle be characterized with alignment methods that use homologous proteins (e.g., [138]) or intrinsic properties of the nucleotide sequence that are learned for instance with Hidden Markov models (e.g., [139]). A radically different approach that has turned out to be even more successful is to model the task of finding TIS as a classification problem (see e.g., [140], [28]). A potential start codon is typically a ATG\textsuperscript{14} triplet. The classification task is therefore to decide whether or not a binary coded (fixed length) sequence window\textsuperscript{15} around the ATG indicates a true TIS. The machine learning algorithm, for example the neural network [140] or the SVM [28] gets a training set consisting of an input of binary coded strings in a window around the ATG together with a label indicating true/false TIS. In contrast to alignment methods, both neural networks and the SVM algorithm are finding important structure in the data by learning in the respective feature space to successfully classify from the labeled data.

As indicated in Section VII-A.1, one can incorporate prior knowledge to SVMs e.g. by using a proper feature space $\mathcal{F}$. In particular in the task of TIS recognition it turned out to be very helpful to include biological knowledge by engineering an appropriate kernel function [28]. We will give three examples for kernels that are particularly useful for start codon recognition. While certain local correlations are typical for TIS, dependencies between distant positions are of minor importance or are a priori known to not even exist. We want the feature space to reflect this. Thus, we modify the kernel utilizing a technique that was originally described for OCR in [131]: At each sequence position, we compare the two sequences locally, within a small window of length $2l + 1$ around that position. We count matching nucleotides, multiplied with weights $p$ increasing from the boundaries to the center of the window. The resulting weighted counts are taken to the $d_k^th$ power.

$$\text{win}_p(x, y) = \left( \sum_{j=-l}^{l} p_j \text{match}_{p+j}(x, y) \right)^{d_k},$$

where $d_k$ reflects the order of local correlations (within the window) that we expect to be of importance. Here, $\text{match}_{p+j}(x, y)$ is 1 for matching nucleotides at position $p + j$ and 0 otherwise. The window scores computed with $\text{win}_p$ are summed over the whole length of the sequence.

\textsuperscript{14}DNA has a four letter alphabet: A, C, G, T.
\textsuperscript{15}We define the input space by the same sparse bit-encoding scheme as used by Pedersen and Nielsen (personal communication): each nucleotide is encoded by five bits, exactly one of which is set. The position of the set bit indicates whether the nucleotide is A, C, G or T, or if it is unknown. This leads to an input space of dimension $n = 1000$ for a symmetric window of size 100 to the left and right of the ATG sequence.

Correlations between up to $d_2$ windows are taken into account by applying potentiation with $d_2$ to the resulting sum.

$$k(x, y) = \left( \sum_{j=1}^{l} \text{win}_p(x, y) \right)^{d_2}.$$ We call this kernel locality-improved (contrary to a plain polynomial kernel), as it emphasizes local correlations.

In an attempt to further improve performance we aimed to incorporate another piece of biological knowledge into the kernel, this time concerning the codon-structure of the coding sequence. A codon is a triplet of adjacent nucleotides that codes for one amino acid. By definition the difference between a true TIS and a pseudo site is that downstream of a TIS there is CDS (which shows codon structure), while upstream there is not. CDS and non-coding sequences show statistically different compositions. It is likely that the SVM exploits this difference for classification. We could hope to improve the kernel by reflecting the fact that CDS shifted by three nucleotides still looks like CDS. Therefore, we further modify the locality-improved kernel function to account for this translation-invariance. In addition to counting matching nucleotides on corresponding positions, we also count matches that are shifted by three positions. We call this kernel codon-improved. Again, it can be shown to be a valid Mercer kernel function by explicitly deriving the monomial features.

\textbf{Table IV}

<table>
<thead>
<tr>
<th>algorithm</th>
<th>parameter setting</th>
<th>overall error</th>
</tr>
</thead>
<tbody>
<tr>
<td>neural network</td>
<td></td>
<td>15.4%</td>
</tr>
<tr>
<td>Salzberg method</td>
<td></td>
<td>13.8%</td>
</tr>
<tr>
<td>SVM, simple polynomial</td>
<td>$d=1$</td>
<td>13.2%</td>
</tr>
<tr>
<td>SVM, locality-improved kernel</td>
<td>$d_1=4, l=4$</td>
<td>11.9%</td>
</tr>
<tr>
<td>SVM, codon-improved kernel</td>
<td>$d_1=2, l=3$</td>
<td>12.2%</td>
</tr>
<tr>
<td>SVM, Salzberg kernel</td>
<td>$d_1=3, l=1$</td>
<td>11.4%</td>
</tr>
</tbody>
</table>

A third direction for the modification of the kernel function is obtained by the Salzberg method, where we essentially represent each data point by a sequence of log odd scores relating, individually for each position, two probabilities: first, how likely the observed nucleotide at that position derives from a true TIS and second, how likely that nucleotide occurs at the given position relative to any ATG triplet. We then proceed analogously to the locality-improved kernel, replacing the sparse bit representation by the sequence of these scores. As expected, this leads to a further increase in classification performance. In the strict sense this is not a kernel but corresponds to preprocessing.

The result of an experimental comparison of SVMs using these kernel functions with other approaches are summa-
rized in Table IV. All results are averages over six data partitions (about 11000 patterns for training and 3000 patterns for testing). SVMs are trained on 8000 data points. An optimal set of model-parameters is selected according to the error on the remaining training data and the average errors on the remaining test set are reported in Table IV. Note that the windows consist of 21 + 1 nucleotides. The NN results are those achieved by Pedersen and Nielsen ([140], personal communication). There, model selection seems to have involved test data, which might lead to slightly over-optimistic performance estimates. Positional conditional preference scores are calculated analogously to Salzberg [141], but extended to the same amount of input data also supplied to the other methods. Note that the performance measure shown depends on the value of the classification function threshold. For SVMs, the thresholds are by-products of the training process; for the Salzberg method, “natural” thresholds are derived from prior probabilities by Bayesian reasoning. Overall error denotes the ratio of false predictions to total predictions. The sensitivity versus specificity trade-off can be controlled by varying the threshold.

In conclusion, all three engineered kernel functions clearly outperform the NN as devised by Pedersen and Nielsen or the Salzberg method by reducing the overall number of misclassifications drastically: up to 25% compared to the neural network.

Further successful applications of SVMs have emerged in the context of gene expression profile analysis [26, 27], DNA and protein analysis [29, 30, 31].

B. Benchmarks

To evaluate a newly designed algorithm it is often desirable to have some standardized benchmark data sets. For this purpose there exists some benchmark repositories, including UCI [142], DELVE [143] and STATLOG [144]. Some of them also provide results of some standard algorithms on these data sets. The problem about these repositories and the given results is that

- it is unclear how the model selection was performed,
- it is not in all cases stated how large the training and test samples have been,
- usually there is no information how reliable these results are (error bars),
- the data sometimes needs preprocessing,
- the problems are often multi-class problems,

Some of these factors might influence the result of the learning machine at hand and makes a comparison with results e.g. in other papers difficult.

Thus, another (very clean) repository – the IDA repository [145] – has been created, which contains thirteen artificial and real world data sets collected from the repositories above. The IDA repository is designed to cover a variety of different data sets: from small to high expected error rates, from low to high dimensional data and from small and large sample sizes. For each of the data sets banana (toy data set introduced in [128], [102]), breast cancer, diabetes, german, heart, image segment, ringnorm, flare solar, splice, thyroid, titanic, twonorm, waveform), the repository includes

- a short description of the dataset,
- 100 predefined splits into training and test samples,
- the simulation results for several kernel based and Boosting methods on each split including the parameters that have been used for each method,
- a simulation summary including means and standard deviations on the 100 realizations of the data.

To build the IDA repository for problems that are originally not binary classification problems, a random partition into two classes is used. Furthermore for all set preprocessing is performed and 100 different partitions into training and test set (mostly $\approx 60\% : 40\%$) have been generated. On each partition a set of different classifiers is trained, the best model is selected by cross-validation and then its test set error is computed. Some of the results are stated in Table V. This repository has been used so far to evaluate kernel and boosting methods e.g. in [128], [102], [89], [7], [129], [130], [97].

In Table V we show experimental comparisons between SVM, RBF, KFD and AdaBoost variants [8]. Due to the careful model selection performed in the experiments, all kernel based methods exhibit a similar good performance. Note that we can expect such a result since they use similar implicit regularization concepts by employing the same kernel [58]. The remaining differences arise from their different loss functions which induce different margin optimization strategies: KFD maximizes the average margin whereas SVM maximizes the soft margin (ultimately the minimum margin). In practice, KFD or RVM have the advantage that – if required (e.g. medical application, motion tracking) – they can also supply a confidence measures for a decision. Furthermore, the solutions for KFD with a sparsity regularization are as sparse as for RVM [91] (i.e. much higher sparsity than for SVMs can be achieved), yet using an order of magnitude less computing time than the RVM [89].

B.1 Miscellaneous Applications

The high dimensional problem of text categorization seems to be another application where SVMs have been performing particularly well. A popular benchmark is the Reuters-21273 text corpus, where Reuters collected 21450 news stories from 1997, and partitioned and indexed them into 135 different categories, to simplify the access. The feature typically used to classify Reuters documents are 10000-dimensional vectors containing word frequencies within a document. With such a coding SVMs have been achieving excellent results, see e.g. [146], [78].

16 The breast cancer domain was obtained from the University Medical Center, Inst. of Oncology, Ljubljana, Yugoslavia. Thanks go to M. Zwitter and M. Soklic for providing the data.

17 A random partition generates a mapping $m$ of $n$ to two classes. For this a random $\pm 1$ vector $m$ of length $n$ is generated. The positive classes (and the negative respectively) are then concatenated.
Further applications of SVM include object and face recognition tasks as well as image retrieval [147], [148]. SVMs have also been successfully applied to solve inverse problems [5], [149].

C. Unsupervised Learning

C.1 Denoising

Kernel PCA as a nonlinear feature extractor has proven powerful as a preprocessing step for classification algorithms. But considering it as a natural generalization of linear PCA the question arises, how to use nonlinear features for data compression, reconstruction, and de-noising, applications common in linear PCA. This is a nontrivial task, as the results provided by kernel PCA live in the high dimensional feature space and need not have an exact representation by a single vector in input space. In practice this issue has been alleviated by computing approximate pre-images [12], [13], [116].

Formally, one defines a projection operator $P_k$ which for each test point $x$ computes the projection onto the first $k$ (nonlinear) principal components, i.e.

$$ P_k \Phi(x) = \sum_{i=1}^{k} \beta_i V_i $$

where $\beta_i := (V_i \cdot \Phi(x)) = \sum_{j=1}^{n} \alpha_j k(x, x_j)$. Lets assume that the Eigenvectors $V$ are ordered with decreasing Eigenvalue size. It can be shown that these projections have similar optimality properties as linear PCA [12] making them good candidates for the following applications:

Denoising. Given a noisy $x$, map it into $\Phi(x)$, discard higher components to obtain $P_k \Phi(x)$, and then compute a pre-image $z$. Here, the hope is that the main structure in the data set is captured in the first $k$ directions, and the remaining components mainly pick up the noise — in this sense, $z$ can be thought of as a denoised version of $x$.

Compression. Given the eigenvectors $\alpha$ and a small number of features $\beta_i$ of $\Phi(x)$, but not $x$, compute a pre-image as an approximate reconstruction of $x$. This is useful if $k$ is smaller than the dimensionality of the input data.

Interpretation. Visualize a nonlinear feature extractor $V'$ by computing a pre-image.

This can be achieved by computing a vector $z$ satisfying $\Phi(z) = P_k \Phi(x)$. The hope is that for the kernel used, such a $z$ will be a good approximation of $x$ in input space. However, (i) such a $z$ will not always exist and (ii) if it exists, it need be not unique (cf. [12], [13]). When the vector $P_k \Phi(x)$ has no pre-image $z$ one can approximate it by minimizing

$$ \rho(z) = \| \Phi(z) - P_k \Phi(x) \|^2, $$

what can be seen as a special case of the reduced set method [150], [13]. The optimization of (29) can be formulated using kernel functions. Especially for RBF kernels (cf. (7)) there exists an efficient fixed-point iteration. For further details of how to optimize (29) and for details of the experiments reported below the reader is referred to [13].

C.1.a Example. The example shown here (taken from [12]) was carried out with Gaussian kernels, minimizing (29). Figure 16 illustrates the pre-image approach in an artificial de-noising task on the USPS database. In these experiments, linear and kernel PCA were trained with the original data. To the test set

(i) additive Gaussian noise with zero mean and standard deviation $\sigma = 0.5$, or

(ii) ‘speckle’ noise, where each pixel is flipped to black or white with probability $p = 0.2$.

was added. For the noisy test sets, projections onto the first $k$ linear and nonlinear components were computed and the reconstruction was carried out for each case. The results were compared by taking the mean squared distance of each reconstructed digit of the noisy test set to its original counterpart.

For the optimal number of components in linear and kernel PCA, the non-linear approach did better by a factor of

<table>
<thead>
<tr>
<th></th>
<th>SVM</th>
<th>KFD</th>
<th>RBF</th>
<th>AB</th>
<th>AB$_R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banana</td>
<td>11.5±0.07</td>
<td>10.8±0.06</td>
<td>10.8±0.06</td>
<td>12.3±0.07</td>
<td>10.9±0.04</td>
</tr>
<tr>
<td>B. Cancer</td>
<td>26.0±0.47</td>
<td>25.8±0.46</td>
<td>27.6±0.47</td>
<td>30.4±0.47</td>
<td>26.5±0.45</td>
</tr>
<tr>
<td>Diabetes</td>
<td>23.5±0.17</td>
<td>23.2±0.16</td>
<td>24.3±0.19</td>
<td>26.5±0.23</td>
<td>23.8±0.18</td>
</tr>
<tr>
<td>German</td>
<td>23.6±0.21</td>
<td>23.7±0.22</td>
<td>24.7±0.24</td>
<td>27.5±0.25</td>
<td>24.3±0.21</td>
</tr>
<tr>
<td>Heart</td>
<td>16.0±0.33</td>
<td>16.1±0.34</td>
<td>17.6±0.33</td>
<td>20.3±0.34</td>
<td>16.5±0.35</td>
</tr>
<tr>
<td>Image</td>
<td>3.0±0.06</td>
<td>3.3±0.06</td>
<td>3.3±0.06</td>
<td>2.7±0.07</td>
<td>2.7±0.06</td>
</tr>
<tr>
<td>Ringnorm</td>
<td>1.7±0.01</td>
<td>1.5±0.01</td>
<td>1.7±0.02</td>
<td>1.9±0.03</td>
<td>1.6±0.01</td>
</tr>
<tr>
<td>F. Sonar</td>
<td>32.4±0.18</td>
<td>33.2±0.17</td>
<td>34.4±0.20</td>
<td>35.7±0.18</td>
<td>34.2±0.22</td>
</tr>
<tr>
<td>Splice</td>
<td>10.9±0.07</td>
<td>10.5±0.06</td>
<td>10.0±0.10</td>
<td>10.1±0.05</td>
<td>9.5±0.07</td>
</tr>
<tr>
<td>Thyroid</td>
<td>4.8±0.22</td>
<td>4.2±0.21</td>
<td>4.5±0.21</td>
<td>4.4±0.22</td>
<td>4.6±0.22</td>
</tr>
<tr>
<td>Titanic</td>
<td>22.4±0.10</td>
<td>23.2±0.20</td>
<td>23.3±0.13</td>
<td>22.6±0.12</td>
<td>22.6±0.12</td>
</tr>
<tr>
<td>Twnorm</td>
<td>3.0±0.02</td>
<td>2.6±0.02</td>
<td>2.9±0.03</td>
<td>3.0±0.03</td>
<td>2.7±0.02</td>
</tr>
<tr>
<td>Waveform</td>
<td>9.9±0.04</td>
<td>9.9±0.04</td>
<td>10.7±0.11</td>
<td>10.8±0.06</td>
<td>9.8±0.08</td>
</tr>
</tbody>
</table>
1.6 for the Gaussian noise, and 1.2 for the ‘speckle’ noise (the optimal number of components were 32 in linear PCA, and 512 and 256 in kernel PCA, respectively). Taking identical numbers of components in both algorithms, kernel PCA becomes up to 8 times better than linear PCA. Recently, in [116] a similar approach was used together with sparse kernel PCA on real world images showing far superior performance compared to linear PCA as well.

Other applications of Kernel PCA can be found in [151] for object detection, and in [4], [119], [152] for preprocessing in regression and classification tasks.

VIII. CONCLUSION AND DISCUSSION

The goal of the present article was to give a simple introduction into the exciting field of kernel based learning methods. We only briefly touched learning theory and feature spaces—omitting many details of VC theory (e.g. [5])—and instead focused on how to use and work with the algorithms. In the supervised learning part, we dealt with classification, however, a similar reasoning leads to algorithms for regression with KFD (e.g. [89]), Boosting (e.g. [108]) or SVMs (e.g. [33]).

We proposed a conceptual framework for KFD, Boosting and SVMs as algorithms that essentially differ in how they handle the high dimensionality of kernel feature spaces. One can think of boosting as a “kernel algorithm” in a space spanned by the basis hypotheses. The problem becomes only tractable since Boosting uses a $\ell_1$-norm regularizer, which induces sparsity, i.e. we essentially only work in a small subspace. In SVMs and KFD, on the other hand, we use the kernel trick to only implicitly work in feature space. The three methods use different optimization strategies, each well suited to maximize the (average) margin in the respective feature space and to achieve sparse solutions.

The unsupervised learning part reviewed (i) kernel PCA, a nonlinear extension of PCA for finding projections that give useful nonlinear descriptors of the data and (ii) the single-class SVM algorithm that estimates the support (or, more generally, quantiles) of a data set and is an elegant approach to the outlier detection problem in high dimensions. Similar unsupervised single-class algorithms can also be constructed for Boosting [110] or KFD.

Selected real-world applications served to exemplify that kernel based learning algorithms are indeed highly competitive on a variety of problems with different characteristics.

To conclude, we would like to encourage the reader to follow the presented methodology of (re-)formulating linear, scalar product based algorithms into nonlinear algorithms to obtain further powerful kernel based learning machines.

REFERENCES


[67] “http://www.boosting.org/,” A collection of references, soft-


Klaus-Robert Müller received the Diplom degree in mathematical physics 1989 and the Ph.D. in theoretical computer science in 1992, both from University of Karlsruhe, Germany. From 1992 to 1994 he worked as a Postdoctoral fellow at GMD FIRST, in Berlin where he started to build up the Intelligent Data Analysis (IDA) group. From 1994 to 1995 he was a European Community STP Research Fellow at University of Tokyo in Prof. Amari’s Lab. From 1996 on he is department head of the IDA group at GMD FIRST in Berlin and since 1999 he holds a joint associate Professor position of GMD and University of Potsdam. He has been lecturing at Humboldt University, Technical University Berlin and University of Potsdam. In 1999 he received the annual national prize for pattern recognition (Olympus Prize) awarded by the German pattern recognition society DAGM. He serves in the editorial board of Computational Statistics, IEEE Transactions on Biomedical Engineering and in program and organization committees of various international conferences. His research areas include statistical physics and statistical learning theory for neural networks, support vector machines and ensemble learning techniques. His present interests are expanded to time-series analysis, blind source separation techniques and to statistical denoising methods for the analysis of biomedical data.

Sebastian Mika is a doctoral student at GMD FIRST (IDA), Berlin. He received the Diplom in computer science from the Technical University of Berlin in 1998. His scientific interests are in the fields of Machine Learning and Kernel methods.

Gunnar Rätsch is a doctoral student at GMD FIRST (IDA), Berlin. He received the Diplom in computer science from the University of Potsdam (Germany) in 1998, along with the prize for the best student of the faculty of Natural Sciences. His scientific interests are in the fields of Boosting and Kernel methods.

Koji Tsuda is a researcher at Electrotechnical Laboratory, Tsukuba, Japan. From 2000 to 2001 he was a visiting researcher at GMD FIRST (IDA), Berlin. He received a Doctor of Engineering in information science from Kyoto University in 1998. His scientific interests are in the fields of Machine learning and Kernel methods.

Bernhard Schölkopf received an M.Sc. in mathematics and the Lionel Cooper Memorial Prize from the University of London in 1992, followed in 1994 by the Diplom in physics from the Eberhard-Karls-Universität, Tübingen, with a thesis written at the Max-Planck-Institute for biological cybernetics. Three years later, he obtained a Ph.D. in computer science from the Technical University Berlin. His thesis on Support Vector Learning won the annual dissertation prize of the German Association for Computer Science (GI) 1997. He has worked at AT&T Bell Labs [with V. Vapnik], at GMD FIRST (IDA), Berlin, at the Australian National University and Microsoft Research Cambridge (UK); currently he is with Barnhill Technologies. He has taught at the Humboldt University and the Technical University Berlin. His scientific interests include machine learning and perception.