Abstract

Machine learning and pattern recognition algorithms have in the past years developed to become a working horse in brain imaging and the computational neurosciences, as they are instrumental for mining vast amounts of neural data of ever increasing measurement precision and detecting minuscule signals from an overwhelming noise floor. They provide the means to decode and characterize task relevant brain states and to distinguish them from non-informative brain signals. While undoubtedly this machinery has helped to gain novel biological insights, it also holds the danger of potential unintentional abuse. Ideally machine learning techniques should be usable for any non-expert, however, unfortunately they are typically not. Overfitting and other pitfalls may occur and lead to spurious and nonsensical interpretation. The goal of this review is therefore to provide an accessible and clear introduction to the strengths and also the inherent dangers of machine learning usage in the neurosciences.

Keywords: pattern recognition, machine learning, model selection, cross validation

1. Introduction

The past years have seen an immense rise of interest in the decoding of brain states as measured invasively with multi-unit arrays and electrocorticography (ECoG) or non-invasively with functional Magnetic Resonance Imaging (fMRI), electroencephalography (EEG), or Near-infrared spectroscopy (NIRS). Instrumental to this development has been the use of modern machine learning and pattern recognition algorithms (e.g. Bishop (1995); Vapnik (1995); Duda et al. (2001); Hastie et al. (2001); Müller et al. (2001); Schölkopf and Smola (2002); Rasmussen and Williams (2005)). Clearly, in this development the field of real-time decoding for brain-computer interfacing (BCI) has been a technology motor (e.g. Dornhege et al. (2007); Kübler and Kotchoubey (2007); Kübler and Müller (2007); Wolpaw (2007); Birbaumer (2006); Pfurtscheller et al. (2005); Curran and Stokes (2003); Wolpaw et al. (2002); Kübler et al. (2001)). As a result a number of novel data driven approaches specific to neuroscience have emerged: (a) dimension reduction and projection methods (e.g. Hyvärinen et al. (2001); Ziehe et al. (2000); Parra and Sajda (2003); Morup et al. (2008); von Bünau et al. (2009); Blanchard et al. (2006); Bießmann et al. (2009)), (b) classification methods (e.g. Müller et al. (2001); Müller et al. (2003); Parra et al. (2002, 2003); Lal et al. (2004); Blankertz et al. (2006a, 2008b); Müller et al. (2008); Parra et al. (2008); Tomioka et al. (2007); Tomioka and Müller (2010)), (c) spatio-temporal filtering algorithms (e.g. Fukunaga (1972); Koles (1991); Ramoser et al. (2000); Lemm et al. (2005); Blankertz et al. (2008b); Dornhege et al. (2006); Tomioka and Müller (2010); Parra et al. (2008); Dornhege et al. (2007); Blankertz et al. (2007)), (d) measures for determining synchrony, coherence or causal relations in data (e.g. Meinecke et al. (2005); Brunner et al. (2006); Nolte et al. (2004); Marzetti et al. (2008); Nolte et al. (2008, 2006); Gentili et al. (2009)) and (e) algorithms for assessing and counteracting non-stationarity in data (e.g. Shenoy et al. (2006); Sugiyama et al. (2007); von Bünau et al. (2009); Blankertz et al. (2008a); Krauledat et al. (2007)). Moreover a new generation of source localization techniques is now in use (e.g. Haufe et al. (2008, 2009)) and has been successfully applied in BCI research (e.g. Pun et al. (2006); Noirhomme et al. (2008); Grosse-Wentrup et al. (2007)).

Despite of this multitude of powerful novel data analytical methods, this review will place its focus mainly
on the essentials for decoding brain states, namely we will introduce the mathematical concept of classification and model selection, and explicate how to properly apply them to neurophysiological data. To this end, the paper first reviews the mathematical and algorithmic principles starting from a rather abstract level and regardless of the scope of application. The subsequent discussion of the practicalities and 'tricks' in the spirit of Orr and Müller (1998) will then link to the analysis of brain imaging data. Unlike existing reviews on this topic (cf. Wolpaw et al. (2002); Kübler and Müller (2007); Dornhege et al. (2007); Haynes and Rees (2006); Pereira et al. (2009)), we will elaborate on common pitfalls and how to avoid them when applying machine learning to brain imaging data.

A final note: while the paper introduces the main ideas of algorithms, we do not attempt a full treatment of the available literature. Rather, we present a somewhat biased view, mainly drawing from the author’s work and providing – to the best of our knowledge – links and reference to related studies and further reading. We sincerely hope that it will nevertheless be useful to the reader.

The paper outline is the following: After a brief introduction, we discuss machine learning principles in Section 2 and then, Section 3 provides feature extraction and dimensionality reduction methods, both supervised and unsupervised. The main contributions of this review are a detailed account of how to validate and select models (Section 4), and the elaboration of the practical aspects of model evaluation and most common pitfalls specific to brain imaging data in Section 5.

2. Learning to classify

Neuroscientific experiments often aim at contrasting specific brain states. Typically, the experimenter chooses a neurophysiological paradigm that maximizes the contrast between the brain states (note that there may be more than two states), while controlling for task unrelated processes. After recording brain imaging data, the goal of analysis is to find significant differences in the spatial and the temporal characteristics of the data contrasting the different states as accurate as possible. While simple statistics such as considering, e.g., grand averages (averaging across trials and subjects) may help for model building, more sophisticated machine learning techniques have become increasingly popular due to their great modeling power. Note that the methods we will presented in this paper are likewise applicable to multivariate fMRI voxel time series, to single trial responses in fMRI or EEG, and brain imaging data from any other spatio-temporal, or spectral domain. Formally, the scenario of discrimination of brain states can be cast into a so-called classification problem, where in a data-driven manner a classifier is computed that partitions a set of observations into subsets with distinct statistical characteristics (see Fig. 1). Note, however, that not only paradigms with known physiological connotation but also novel scenarios can be scrutinized, where (1) a new paradigm can be explored with respect to its neurophysiological signatures, (2) a hypothesis about underlying task relevant brain processes is generated automatically by the learning machine. Feeding this information back to the experimenter, may lead to a refinement of the initial paradigm, such that, in principle, a better understanding of the brain processes may follow. In this sense, machine learning may not only be the technology of choice for a generic modeling of a neuroscientific experiment, it can also be of great use in a semi-automatic exploration loop for testing new neurophysiological paradigms.

2.1. Some theoretical background

Let us start with the general notion of the learning problems that we consider in this paper. A classifier is a function which partitions a set of objects into several classes, for instance, recordings of brain activity during either auditory, visual, or cognitive processing into the
three distinct modalities (classes)\(^1\). Thus, based on a set of observations, the machine learning task of classification is to find a rule, which assigns an observation \(x\) to one of several classes. Here, \(x\) denotes a vector of \(N\)-dimensional neuroimaging data. In the simplest case there are only two different classes. Hence, a classifier can be formalized as a decision function \(f: \mathbb{R}^N \rightarrow \{-1, +1\}\), that assigns an observation \(x\) to one of the classes, denoted by \(-1\) and \(1\), respectively. Typically, the set of possible decision functions \(f\) is constrained by the scientist to a (parameterized) class of functions \(\mathcal{F}\), e.g., to the class of linear functions. Note, a linear decision function \(f\) corresponds to a separating hyperplane (e.g., see Fig. 1), that is parameterized by its normal vector \(w\) and a bias term \(b\). Here, the label \(y\) is predicted through

\[
y = f(x; w, b) = \text{sgn}(w^\top x + b).
\]

Then, based on a set of observed input-output relation \((x_1, y_1), \ldots, (x_n, y_n) \in \mathbb{R}^N \times \{-1, +1\}\), learning can be formally described as the task of selecting the parameter value \((w, b)\) and hence selecting the decision function \(f \in \mathcal{F}\) such that \(f\) will correctly classify unseen examples \(x\). Here, the observed data \((x_i, y_i)\) is assumed to be independently and identically distributed (i.i.d.) according to an unknown distribution \(P(x, y)\) that reflects the relationship between the objects \(x\) and the class labels \(y\), e.g., between the recorded brain activity and the paradigm specific mental states. However, in order to find the optimal decision function one needs to specify a suitable loss function that evaluates the goodness of the partitioning. One of the most commonly used loss functions for classification is the so-called 0/1-loss (see Smola and Schölkopf (1998) for a discussion of other loss functions)

\[
l(y, f(x)) = \begin{cases} 0 & y = f(x) \\ 1 & \text{else} \end{cases}
\]

Given a particular loss function, the best decision function \(f\) one can obtain, is the one minimizing the expected risk (also often called generalization error)

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

under the unknown distribution \(P(x, y)\). As the underlying probability distribution \(P(x, y)\) is unknown the expected risk cannot be minimized directly. Therefore, we have to try to estimate the minimum of (2.3) based on the information available, such as the training sample and properties of the function class \(\mathcal{F}\). A straightforward approach is to approximate the risk in (2.3) by the empirical risk, i.e., the averaged loss on the training sample

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

and minimize the empirical risk with respect to \(f\). It is possible to give conditions on the learning machine which ensure that asymptotically (as the number of observations \(n \rightarrow \infty\) the minimum of the empirical risk will converge towards the one of the expected risk. Consequently, with an infinite amount of data the decision function \(f\) that minimizes the empirical risk will also minimize the expected risk. However, for small sample sizes this approximation is rather coarse and large deviations are possible. As a consequence of this, overfitting might occur, where the decision function \(f\) learns details of the sample rather than global properties of \(P(x, y)\) (see Fig. 2 and 4).

![Figure 2: Illustration of the overfitting dilemma](image)

Under such circumstances, simply minimizing the empirical error (2.4) will not yield a small generalization error in general. One way to avoid the overfitting dilemma is to restrict the complexity of the function \(f\) Vapnik (1995). 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 over a complex one (Occam’s razor, cf. MacKay (2003)). This is typically realized by adding a regularization term (e.g., Kimeldorf and Wahba (1971); Tikhonov and Arsenin (1977); Poggio and Girosi (1990); Cox and O’Sullivan (1990)) to the empirical risk, i.e.,

\[
R_{\text{reg}}[f] = R_{\text{emp}} + \lambda \|f\|^2.
\]

Here, an appropriately chosen regularization operator \(\|f\|^2\) penalizes high complexity or other undesired

\(^1\)The classes could also correspond to complex brain states as in mind reading paradigms (see Haynes and Rees (2006)) or brain states such as attention, workload, emotions, etc.
properties of a function $f$; $\lambda$ introduces an additional parameter to the model (often called hyperparameter) that needs to be estimated as well. The estimation of this parameter and hence taking model complexity into account, raises the problem of model selection (e.g., Akaike (1974); Poggio and Girosi (1990); Moody (1992); Murata et al. (1994)), i.e., how to find the optimal complexity of a function or accordingly the appropriate function class (in Section 4 we will discuss the practical aspects of model selection). As a brief remark, Linear Discriminant Analysis (LDA) employs regularization through shrinkage (Stein (1956); Friedman (1989)) while neural networks use early stopping (Amari et al. (1997)), weight decay regularization or asymptotic model selection criteria (e.g., network information criterion (Murata et al. (1994); Akaike (1974)), see also (Bishop (1995); Orr and Müller (1998))). On the other hand, support vector machines (SVMs) regularize according to what kernel is being used (Smola et al. (1998)) and limit their capacity according to Vapnik-Chervonenkis (VC) theory (Vapnik (1995)). We will now briefly outline a few algorithms.

**Figure 3**: Schematic illustration of model selection. The solid line represents the empirical error, the dashed line the expected error. With higher complexity, the ability of the model to overfit the sample data increases, visible from a low empirical and an increasing expected error. The task of model selection is to determine the model with the smallest generalization error.

### 2.2. Linear Classification

For computing the parameters of a linear decision function (cf. (2.1) and Fig. 1), namely the normal vector $w$ and the bias $b$, we will in the following discuss different linear methods: Linear Discriminant Analysis (LDA) including procedures for regularizing LDA, as well as linear programming machines (LPM).

#### 2.2.1. Linear Discriminant Analysis, Fisher’s Discriminant and Regularization

In case of LDA the two classes are assumed to be normally distributed with different means but identical full rank covariance matrix. Suppose the true means $\mu_i$ (i=1,2) and the true covariance matrix $\Sigma$ are known, then the normal vector $w$ of the Bayes optimal separating hyperplane of the LDA classifier is given as

$$w = \Sigma^{-1}(\mu_1 - \mu_2).$$

In order to compute $w$ for real data, the means and covariances need to be approximated empirically, see Section 2.2.2.

A more general framework is the well-known Fisher’s Discriminant analysis (FDA), that maximizes the so-called Rayleigh coefficient

$$J(w) = \frac{w^T S_B w}{w^T S_w w},$$

where the within class scatter $S_w = \sum_{i=1}^c S_i$ with $S_i = \sum_{x \in C_i} (x - \mu_i)(x - \mu_i)^T$ and the class means are defined as $\mu_i = \frac{1}{n_i} \sum_{x \in C_i} x$ and $n_i$ is the number of patterns $x_i$ in class $C_i$. The between class scatter $S_B = 1/2 \sum_{i=1}^c (\mu_i - \mu)(\mu_i - \mu)^T$, where $\mu = 1/2 \sum_{i=1}^c \mu_i$. A solution to (2.6) can be found by solving the generalized Eigenvalue problem (cf. Golub and van Loan (1996)). Considering only two classes, FDA and LDA can be shown to yield the same classifier solution. However, both methods can be extended for the application to multiple classes.

Although it is a common wisdom that linear methods such as LDA and FDA are less likely to overfit, we would like to stress that they also require careful regularization: not only for numerical reasons. Here, the regularization procedure will be less necessary to avoid the typical overfitting problems due to excessive complexity encountered for nonlinear methods (see Fig. 2 and Fig. 4-right). Rather regularization will help to limit the influence of outliers that can distort linear models (see Fig. 4-center). However, if possible, a removal of outliers prior to learning is to be preferred (e.g., Schölkopf et al. (2001); Harmeling et al. (2006)).

A mathematical programming formulation of regularized Fisher Discriminant analysis (RFDA) as a linear constrained, convex optimization problem was introduced in Mika et al. (2001) as

$$\text{min}_{w,b,\xi} \frac{1}{2} ||w||_2^2 + \frac{C}{n} ||\xi||_2^2$$

s.t. $y_i \cdot ((w^T x_i) + b) = 1 - \xi_i$, $i = 1, \ldots, n$

$\xi_i \geq 0,$

where $||w||_2$ denotes the 2-norm (i.e., $||w||_2 = w^T w$) and $C$ is a model parameter that controls for the amount of constraint violations introduced by the slack variables $\xi_i$. The constraints $y_i \cdot ((w^T x_i) + b) = 1 - \xi_i$ ensure that
the class means are projected to the corresponding class labels \( \pm 1 \). Minimizing the length of \( w \) maximizes the margin between the projected class means relative to the intra class variance. Note that (2.8) can be the starting point for further mathematical program formulations of classifiers such as the sparse FDA, which uses an 1-norm regularizer: \( \|w\|_1 = \sum |w_j| \) etc. (cf. Mika et al. (2003)).

Then the following holds: \( \hat{\Sigma} \) and \( \hat{\Sigma} \) have the same Eigenvectors; extreme eigenvalues (large or small) are modified (shrunk or elongated) towards the average \( v \); \( \gamma = 0 \) yields unregularized LDA, \( \gamma = 1 \) assumes spherical covariance matrices.

Using LDA with such a modified covariance matrix is termed regularized LDA or LDA with shrinkage. For a long time, complex or time-consuming methods have been used to select shrinkage parameter \( \gamma \), e.g., by means of cross validation. Recently an analytic method to calculate the optimal shrinkage parameter for certain directions of shrinkage was found (Ledoit and Wolf (2004); see also Vidaurre et al. (2009) for the first application to brain imaging data) that is surprisingly simple. The optimal value only depends on the sample-to-sample variance of entries in the empirical covariance matrix (and values of \( \hat{\Sigma} \) itself). When we denote by \((x_i, \mu_i)\) the \( i \)-th element of the vector \( x \) and \( \mu_i \), respectively and denote by \( s_i \) the element in the \( i \)-th row and \( j \)-th column of \( \Sigma \) and define

\[
z_{ij}(k) = ((x_i) - (\mu_i))((x_k) - (\mu_k)),
\]

then the optimal parameter \( \gamma \) for shrinkage towards identity (as defined by (2.8)) can be calculated as (Schäfer and Strimmer (2005))

\[
\gamma^* = \frac{n}{(n - 1)^2} \frac{\sum_{i,j=1}^{d} \text{var}_{x_i}(z_{ij}(k))}{\sum_{i,j} s_{ij}^2 + \sum (s_{ii} - v)^2}.
\]

2.2.2. Linear Discriminant Analysis with Shrinkage

The optimality statement for LDA depends crucially on the never fulfilled assumption, that the true class distributions are known. Rather, means and covariance matrices of the distributions have to be estimated from the training data.

The standard estimator for a covariance matrix is the empirical covariance which is unbiased and has under usual conditions good properties. But for extreme cases of high-dimensional data with only a few data points that is typically encountered in neuroimaging data, the empirical estimation may become imprecise, because the number of unknown parameters that have to be estimated is quadratic in the number of dimensions. As substantiated in Blankertz et al. (2010), this results in a systematic error: Large eigenvalues of the original covariance matrix are estimated too large, and small eigenvalues are estimated too small. Shrinkage is a common remedy for the systematic bias (Stein (1956)) of the estimated covariance matrices (e.g., Friedman (1989)): the empirical covariance matrix \( \Sigma \) is replaced by

\[
(2.8) \quad \hat{\Sigma}(\gamma) := (1 - \gamma)\Sigma + \gamma v I
\]

for a tuning parameter \( \gamma \in [0, 1] \) and \( v \) defined as average eigenvalue of \( \hat{\Sigma} \) and \( I \) being the identity matrix.

Figure 4: The problem of finding a maximum margin “hyper-plane” on reliable data (left), data with outlier (middle) and with a mislabeled pattern (right). The solid line shows the resulting decision line, whereas the dashed line marks the margin area. In the middle and on the left the original decision line is plotted with dots. The hard margin implies noise sensitivity, because only one pattern can spoil the whole estimation of the decision line. Figure from Rätsch et al. (2001).

2.2.3. Linear Programming Machines

Finally, we would like to introduce so-called Linear Programming Machines (LPMs, Bennett and Mangasarian (1992); Tibshirani (1994, 1996); Hastie et al. (2001); Müller et al. (2001); Rätsch et al. (2002)). Here, slack variables \( \xi \) corresponding to the estimation error incurred as well as parameters \( w \) are optimized to yield a sparse regularized solution

\[
(2.9) \quad \min_{w,b,\xi} \frac{1}{2} \|w\|_1 + \frac{C}{n} \|\xi\|_1 \quad \text{s.t.} \quad y_i ((w^T x_i) + b) \geq 1 - \xi_i, \quad i = 1, \ldots, n \quad \xi_i \geq 0.
\]

LPMs achieve sparse solutions (i.e. most values of \( w \) become zero) by means of explicitly optimizing the 1-norm in the objective function instead of the 2-norm, which is known to yield non-sparse solutions. Due to this property, LPM and sparse FDA are excellent tools for variable selection. In other words, while solving the classification problem, the user is not only supplied with a good classifier but also with the list of variables that are relevant for solving the classification task (Blankertz et al. 2006).
et al. (2006a); Müller et al. (2001); Blankertz et al. (2002); Lal et al. (2004); Tomioka and Müller (2010)).

2.3 Beyond linear classifiers

Kernel based learning has taken the step from linear to nonlinear classification in a particularly interesting and efficient manner: a linear algorithm is applied in some appropriate (kernel) feature space. While this idea first described in Schölkopf et al. (1998) is simple, it is yet very powerful as all beneficial properties (e.g., optimality) of linear classification are maintained, but at the same time the overall classification is nonlinear in input space, since feature- and input space are nonlinearly related.

A cartoon of this idea can be found in Fig. 5, where the classification in input space requires some complicated non-linear (multi-parameter) ellipsoid classifier. An appropriate feature space representation, in this case polynomials of second order, supply a convenient basis in which the problem can be most easily solved by a linear classifier.

However, by virtue of the kernel-trick the input space does not need to be explicitly mapped to a high dimensional feature space by means of a non-linear function $\Phi : x \mapsto \Phi(x)$. Instead, kernel based methods take advantage from the fact that most linear methods only require the computation of dot products. Hence, the trick in kernel based learning is to substitute an appropriate kernel function in the input space for the dot products, i.e.,

$$ k : \mathbb{R}^N \times \mathbb{R}^N \rightarrow \mathbb{R}, $$

such that $k(x, x') = \phi(x)\top\phi(x')$.

More precisely, kernel-based methods restrict to the particular class of kernel functions $k$ that correspond to dot products in feature spaces and hence only implicitly maps the input space to the corresponding feature space. Commonly used kernels are for instance:

$$ k(x, x') = \exp \left(-\frac{||x-x'||^2}{2\sigma^2}\right), \quad \sigma > 0 $$

(2.11) **Gaussian**

$$ k(x, x') = (x^\top x' + c)^d $$

(2.12) **Polynomial**

$$ k(x, x') = \tanh(\kappa(x^\top x') + \theta), \quad \kappa > 0, \theta < 0 $$

(2.13) **Sigmoid**

Examples of kernel-based learning machines are among others, e.g., Support Vector Machines (SVMs) (Vapnik (1995); Müller et al. (2001)), Kernel Fisher Discriminant (Mika et al. (2003)) or Kernel Principal Component Analysis (Schölkopf et al. (1998)).

![Figure 5: Two dimensional classification example. Using the second order monomials $x_1^2$, $\sqrt{2}x_1x_2$ and $x_2^2$ as features a separation in feature space can be found using a linear hyperplane (right). In input space this construction corresponds to a non-linear ellipsoidal decision boundary (left). From Müller et al. (2001).](image)

2.4 Support Vector Machines

In order to illustrate the application of the kernel-trick, let us consider the example of the SVM (Vapnik (1995); Müller et al. (2001)). Here, the primal optimization problem of a linear SVM is given similar to (2.7) and (2.9) as

$$ \begin{align*}
\min_{w, b, \xi} & \quad \frac{1}{2} ||w||_2^2 + C \sum_{i=1}^{n} \xi_i \\
\text{s.t.} & \quad y_i \cdot ((w^\top x_i) + b) \geq 1 - \xi_i, \ i = 1, \ldots, n \\
& \quad \xi_i \geq 0.
\end{align*} $$

(2.14)

However, in order to apply the kernel trick we rather use the dual of (2.14), i.e.,

$$ \begin{align*}
\max_{\alpha} & \quad \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} \alpha_i \alpha_j y_i y_j \cdot (x_i^\top x_j) \\
\text{s.t.} & \quad C \geq \alpha_i \geq 0, \ i = 1, \ldots, n, \\
& \quad \sum_{i=1}^{n} \alpha_i y_i = 0.
\end{align*} $$

(2.15)

To construct a nonlinear SVM in the input space, one (implicitly) maps the inputs $x$ to the feature space by a non-linear feature map $\Phi(x)$ and computes an optimal hyperplane (with threshold) in feature space. To this end, one substitutes $\Phi(x_i)$ for each training example $x_i$ in (2.15). As the $x_i$ only occur in dot products, one can apply the kernel trick and substitute a kernel $k$ for the dot products, i.e., $k(x_i, x_j) = \Phi(x_i)\top\Phi(x_j)$ (cf. Boser et al. (1992); Guyon et al. (1993)). Hence, the non-linear formulation of the SVM is identical to
(2.15), with the exception that the kernel \( k(x_i, x_j) \) substitutes for the dot \( (x_i^\top x_j) \). Advantageously, many of the \( \alpha_i \) will be vanishing; the samples associated with these non-zero coefficients are referred to as support vectors (SV). As the weight vector \( w \) in the primal formulation reads \( w = \sum_y y_i \alpha_i \Phi(x_i) \), we obtain the nonlinear decision function as

\[
f(x) = \text{sgn} \left( w^\top \Phi(x) + b \right) = \text{sgn} \left( \sum_{i, \alpha_i \neq 0} y_i \alpha_i \cdot \left( \Phi(x_i)^\top \Phi(x) \right) + b \right)
\]

(2.16) \[= \text{sgn} \left( \sum_{i, \alpha_i \neq 0} y_i \alpha_i \cdot k(x_i, x) + b \right)\]

Here, the sum in (2.16) is a sparse expansion as it only runs over the set of SVs. Note, while the \( \alpha_i \) are determined from quadratic optimization problem \(^4\) (2.15), the threshold \( b \) can be computed by exploiting the fact that for all support vectors \( x_i \) with \( C \geq \alpha_i \geq 0 \), the slack variable \( \xi_i \) is zero, and hence

\[
2.6. 
\sum_{j=1}^n y_j \alpha_j \cdot k(x_i, x_j) + b = y_i.
\]

If one uses an optimizer that works with the double dual (see, e.g., Vanderbei and Shanno (1997); Boyd and Vandenberghe (2004)), one can also recover the value of the primal variable \( b \) directly from the corresponding double dual variable.

Note that recently Braun et al. (2008) has observed that the excellent generalization that is typically observed when using SVMs in high dimensional applications with few samples is due to its very economic representation in Kernel Hilbert space. Given the appropriate kernel, only a very low dimensional subspace is task relevant.

2.5. \textit{k-nearest neighbors}

A further well-known non-linear algorithm for classification is the so-called \( k \)-nearest neighbor method. Here, every unsewn point \( x \) is compared through a distance function \( \text{dist}(x, x_i) \) to all points \( x_i \) \((i = 1, \ldots, n)\) of the training set. The \( k \) minimal distances are computed and the majority over the corresponding labels \( y_i \) is taken as a resulting label for \( x \) (note that this simple rule also holds for multiclass problems). This strategy provides a very simple local approximation of the conditional density function. The \( k \)-nearest neighbor method is known to work well, if a reasonable distance (typically the Euclidean one) is available and if the number of data points in the training set is not huge. The hyperparameter \( k \) can be selected, e.g., by cross-validation; if the data is noisy a large \( k \) should be chosen.

2.6. Application to brain imaging data

The predominant methods both for fMRI and EEG/MEG analysis are so far mostly linear, however, nonlinear methods can easily be included in the analysis by including these model classes into the model selection loop, as we will discuss in a later section in detail. For a brief discussion of linear versus nonlinear methods see, e.g., Müller et al. (2003).

In EEG studies mainly LDA, shrinkage/regularized LDA, sparse Fisher, and linear programs are in use (e.g., Dornhege et al. (2007)) are in use. Here, it was observed that through a proper preprocessing the class conditional distributions become Gaussian with a very similar covariance structure (cf. Blankertz et al. (2002, 2006a); Dornhege et al. (2007)). Under such circumstances, theory suggests that LDA would be the optimal classifier. However, changes in the underlying distribution, the use of multimodal features (e.g., Dornhege et al. (2004)), or the presence of outliers may require to proceed to nonlinear methods (see the discussion in Müller et al. (2003)).

The driving insight in fMRI analysis was to go from univariate analysis tools that correlate single voxels with behavior to a full multivariate correlation analysis (e.g., Hansen et al. (1999); Hanby and et al (2001); Strother et al. (2002); Cox and Savoy (2003); Kamitani and Tong (2005); Haynes and Rees (2006); Kriegeskorte et al. (2006); Mitchell et al. (2008)). A main argument for using especially SVMs and LPMs was their well-known benign properties in the case where the number of input dimensions in \( x \) is high while the number of samples is low (e.g., Vapnik (1995); Müller et al. (2001); Braun et al. (2008)). This particular very unbalanced situation is an important issue in fMRI, since the number of voxels is of the order ten-thousands while the number of samples rarely exceeds a few hundreds (e.g., Hansen et al. (1999); Strother et al. (2002); Cox and Savoy (2003)). Physiological priors that allow, e.g., to define regions of interest, have led to further specialized analysis tools like the search-light method. Here, the signal to noise ratio is improved by discarding some potentially noisy and task unrelated areas while enhancing the interesting bit of information spatially (e.g., Kriegeskorte et al. (2006)). In some cases improvements through the use of nonlinear kernel functions have been reported, e.g., LaConte et al. (2005) studied polynomial kernels.

\(^4\)A selection of Open Source software for SVMs can be found on \texttt{www.kernel-machines.org}.\[7\]
Other priors have been derived from the paradigm. For example, for understanding the neural basis of word representation, Mitchell et al. (2008) used word co-occurrences in language inferred from a large scale document corpus, to derive a codebook of fMRI patterns corresponding to brain activity for representing words. These patterns could be superimposed for out of sample forecasting, thus predicting the most probable way a certain novel word is represented in the fMRI pattern.

3. Dimensionality Reduction

So far, we did not much concern about the domain of the input data and solely assumed the classifiers to be applicable to the data \((x, y)\). In practice and particularly in the domain of computational neuroscience, the input data \(x\) often exhibit an adverse ratio between its dimensionality and the number of samples. For example, a typical a common task for EEG-based Brain-Computer Interfaces (BCI) requires the classification of one second intervals of brain activity, recorded at sampling frequencies up to 1 kHz, from possibly 128 electrodes. Hence, the dimensionality of the input data \(x\) amounts approximately to \(10^5\), while the number of training samples is typically rather small, up to a few hundred samples. Moreover, the data is contaminated by various sources of interfering noise, while the discriminative information that is the task relevant part of the data is often concentrated in a low dimensional subspace. Consequently, in order to make the classification task feasible the dimensionality of the data needs to be significantly reduced, and informative features have to be extracted (see also Fig. 1). Thus, feature extraction likewise involves spatial, spectral, and temporal preprocessing of the input.

Nevertheless, the extraction of relevant features is a highly paradigm specific task and also differs for the various recording techniques due to their temporal and spatial resolutions. Moreover, the extraction of task relevant features should be facilitated by incorporating prior neurophysiological knowledge, e.g., about the cognitive processes underlying the specific paradigm. In return, purely data driven feature extraction methods can potentially provide new findings about the involved cognitive processing and might therefore contribute to the generation of neurophysiological hypotheses (Blankertz et al. (2006a)). Thus, feature extraction has to be considered not just as a data analytical but rather as a heavily interdisciplinary endeavor.

The common approaches for dimensionality reduction can be subdivided into two main categories. On the one hand side there are variants of factor models, such as the well-known Principle Component Analysis (PCA), Independent Component Analysis (ICA) (cf. Comon (1994); Bell and Sejnowski (1995); Ziehe and Müller (1998); Hyvärinen et al. (2001)), non-negative matrix factorization, archetypal analysis, sparse PCA (Lee and Seung (2000); Zou et al. (2004); Schölkopf et al. (1998)) or Non-Gaussian Component Analysis (Blanchard et al. (2006)); that perform a factorization of the input data \(x\) in a purely unsupervised manner, i.e., without using the class information. The application of these methods serves several purposes (a) dimensionality reduction by projecting onto a few (meaningful) factors, (b) removal of interfering noise from the data to increase the signal-to-noise ratio of the signals of interest, (c) removal of nonstationary effects in data or (d) grouping of effects. Notwithstanding their general applicability, unsupervised factor analysis often requires manual identification of the factors of interest.

The second class of methods, namely supervised methods, make explicit use of the class labels in order to find a transformation of the input data to a reduced set of features with high task relevance. For example, the Common Spatial Pattern (CSP) (cf. Fukunaga (1972); Koles (1991); Ramoser et al. (2000)) algorithm and derivatives thereof (Blankertz et al. (2008b); Lemm et al. (2005); Dornhege et al. (2006); Tomioka and Müller (2010)) is widely used to extract discriminative oscillatory features.

In the following, we will briefly describe two frequently used dimensionality reduction methods. First we will briefly introduce the unsupervised Independent Component Analysis, and subsequently discuss the supervised CSP algorithm.

3.1. Independent component analysis

Under the often valid assumption that the electric fields of different bioelectric current sources superim-
pose linearly, the measured neurophysiological data can be modeled as a linear combination of component vectors. For instance, in case of independent component analysis (ICA) it is assumed that the observed signals $x(t)$ are a linear mixture of $M \leq N$ mutually independent sources $s(t)$, i.e., data are modeled as a linear combination of component vectors:

$$x(t) = As(t),$$

(3.18)

where $A \in \mathbb{R}^{N \times M}$ denotes the linear mixing matrix. In this case (3.18) is invertible and ICA decomposes the observed data $x(t)$ into independent components $y(t)$ by estimating the inverse decomposition matrix $W \approx A^{-1}$, such that $y(t) = Wx(t)$.

There exists a vast number of ICA algorithms that can solve the task of estimating the mixing matrix $A$. They only differ in the particular choice of a so-called index function and the respective numerical procedures to optimize this function. In general, the index function employs a statistical property that takes on its extreme values if the projected sources are independent. Most research conducted in the field of ICA uses higher-order statistics for the estimation of the independent components (Comon (1994); Hyvärinen et al. (2001)). For instance, the Jade algorithm (Cardoso and Souloumiac (1993)) is based on the joint diagonalization of matrices obtained from "parallel slices" of the 4th-order cumulant tensor. Although this algorithm performs very efficiently on low dimensional data, it becomes computationally infeasible for high dimensional problems, as the effort for storing and processing the 4th-order cumulants is $O(m^4)$ in the number of sources. As a remedy for this problem Hyvärinen and Oja (1997) developed a general fix-point iteration algorithm termed FastICA, that optimizes a contrast function measuring the distance of the source probability distributions from a Gaussian distribution.

Note that ICA can recover the original sources $s(t)$ only up to scaling and permutation. Fig. 6 sketches the essential difference between ICA and the well known PCA method.

3.2. Common spatial pattern

Unlike unsupervised methods such as PCA and ICA, the common spatial pattern (CSP) algorithm (Fukunaga (1972)) makes explicit use of the label information in order to calculate discriminative spatial filters that emphasize differences in signal power of oscillatory processes (Koles and Soong (1998)). To illustrate the basic idea of CSP: suppose we observe two class distributions in a high-dimensional space, the CSP algorithm finds directions (spatial filters) that maximize the signal variance for one class, while simultaneously minimizing the signal variance for the opposite class.

To be more precise, let $\Sigma_1$ and $\Sigma_2$ denote the two class conditional signal covariance matrices. The spatial CSP filters $w$ are obtained as the generalized Eigenvectors of the following system

$$\Sigma_1 = \lambda \Sigma_2 w,$$

(3.19)

A solution to (3.19) is typically derived in two steps: first the data are whitened with respect to the mutual covariance matrix $\Sigma_1 + \Sigma_2$; secondly a terminal rotation aligns the principal axes with the coordinate axes (see Fig. 7). However, the interpretation of filter matrix $W$ is two-fold, the rows of $W$ are the spatial filters, whereas the columns of $W^{-1}$ can be seen as the common spatial patterns, i.e., the time-invariant coupling coefficients of each source with the different sensors. For a detailed discussion on the relation between spatial patterns and spatial filters see (Blankertz et al. (2010)).

Originally the CSP algorithm was conceived for discriminating between two classes, but has also been extended to multi-class problems (Dornhege et al. (2004); Grosse-Wentrup and Buss (2008)). Further extension of CSP were proposed in Lemm et al. (2005); Dornhege et al. (2006); Tomioka and Müller (2010); Farquhar (2009); Li and Guan (2006) with the goal of simultaneously optimizing discriminative spatial and spectral filters. For a comprehensive overview of optimizing spatial filters we refer to Blankertz et al. (2008b).

4. Cross-validation and Model selection

Given the data sample, the task of model selection is to choose a statistical model from a set of potential models (the function class), which may have produced the data with maximum likelihood, i.e., to choose the model which resembles the underlying functional relationship.
best. The set of potential models is in general not restricted, although in practice limitations are imposed by the preselection of a model class by the scientists. A typical setting may, for example, comprise models from distinct classes, such as linear and non-linear models; but may also solely consist of non-linear models that differ in the employed SV-kernel function which needs to be selected. On the other hand, model selection is also frequently used to determine the optimal value of model hyperparameters\(^5\). However, in all these cases the general task remains the same: the expected out-of-sample performances of the different models need to be evaluated on the common basis of the given data sample.

As discussed previously, complex models can potentially better adapt to details of the data. On the other hand an excessively complex model will tend to overfit, i.e., will rather fit to the noise than to the underlying functional relationship. Hence, its out-of-sample performance will deteriorate (see Fig. 2 for an illustration of overfitting). However, overfitting not only occurs when a model has too many degrees of freedom, in relation to the amount of data available. Also simple models tend to overfit, if the influence of outliers is not treated appropriately (see Fig. 4). However, in any case the training error does not provide an unbiased estimate of the model performance and hence can not be used to select the best model.

At this point we would like to stress, that an unbiased estimation of the model performance is one of the most fundamental issues in statistical data analysis, as it provides the answer to: How will the model generalize on new, previously unseen data and hence how accurately it will perform in practice. In terms of machine learning, this quantity is called the generalization error or expected risk of a model (cf. (2.3)), which applies likewise to a regression or classification model. So model selection in essence reduces to reliably estimating the ability of a model to generalize well to new unseen data and to pick the model with the smallest expected error (see Fig. 3).

4.1. Estimation of the Generalization Error

In order to present a universally applicable conceptual framework of estimating the generalization error, let \(D = \{(x_1,y_1), \ldots, (x_n,y_n)\}\) represent our original sample set of \(n\) labeled instances. Moreover, let \(f(c|D)\) be the model that has been learned on the sample set and correspondingly \(f(x|D)\) denotes the model prediction at the instance \(x\). Suppose further that the error of the model at an instance \((x,y)\) from the sample space is measured by a given loss function \(err = l(y, f(x|D))\), e.g., by the mean squared error, or the 0/1-loss as it is commonly used for classification. Based on this notation, we will introduce the prevalent concepts for assessing the generalization error of a statistical model given a sample set. All of the following concepts have in common that they are based on a holdout strategy.

A holdout strategy generally splits the sample set in two independent, complementary subsets. One subset, commonly referred to as training set, is solely used for fitting the model, i.e., to estimate the model parameters, such as, the normal vector of the separating hyperplane of an SVM. In contrast, the second subset is exclusively used for the purpose of validating the estimated model on an independent data set and is therefore termed validation set. Formally, let \(D_v \subset D\) denote the holdout validation set of size \(n_v\), and define \(D_t = D \setminus D_v\) as the complementary sample set for training. The estimated validation error is defined as

\[
\text{err}_v = \frac{1}{n_v} \sum_{x \in D_v} l(y, f(x|D_v)).
\]

Note, the learned model as well as the accuracy of the estimated generalization error will depend on the particularly chosen partition of the original sample into training and validation set and especially on the size of these sets. For example, the more instances we leave for validation, the less samples remain for training and hence the model becomes less accurate. Consequently, a bias is introduced to the estimated model error. On the contrary, using fewer instances for validating the model will increase the variance of the estimated model error.

4.1.1. Cross-validation

To trade off between bias and variance several approaches have been proposed. On the one hand side, there is a multitude of cross-validation (CV) schemes, where the process of splitting the sample in two is repeated several times using different partitions of the sample data. Subsequently, the resulting validation errors are averaged across the multiple rounds of CV. The miscellaneous CV schemes differ by the way they split the sample data in two. The most widely used method is \(K\)-fold CV. Here, the sample data is randomly divided into \(K\) disjoint subsets \(D_1, \ldots, D_K\) of approximately equal size. The model is then trained \(K\) times, using all of the data subsamples except for one, which is left out as validation set. In particular, in the \(k\)-th run \(D_k\)

\(^5\)This might simultaneously be the regularization strength \(C\) of a SVM and kernel width \(\sigma\) of say a Gaussian kernel.
is selected as validation set, while the union of the remaining $K-1$ subsamples, i.e., $\mathcal{D} \setminus \mathcal{D}_b$ serves as training set. The $K$-fold CV-error is then the averaged error of the $K$ estimated models, where each model is evaluated separately on its corresponding validation set

$$\text{errs}_k = \frac{1}{n} \sum_{i=1}^{n} l(y_i, f(x_i | \mathcal{D} \setminus \mathcal{D}_b)).$$

Note, that the cross-validation error is still a random number that depends on the particular partition of the data into the $K$ folds. Therefore, it would be highly desirable to perform a complete $K$-fold CV to estimate its mean and variance by averaging across all possible partitions of the data into $K$ folds. In practice this is computationally intractable even for small samples. Nevertheless, repeating the $K$-fold cross-validation several times can additionally reduce the variance of the estimator at lower computational costs.

An alternative cross-validation scheme is the so-called leave-one-out cross-validation (LOO-CV). As the name already indicates, LOO-CV uses all but a single data point of the original sample for training the model. The estimated model is then validated on the single observation left out. This procedure is repeated, until each data point once served as validation set. In particular, in the $i$-th run the validation set corresponds to $\mathcal{D}_b = (x_i, y_i)$, while the model is trained on the complement $\mathcal{D} \setminus \mathcal{D}_b$. The LOO-CV estimator is defined as the averaged error

$$\text{err}_{LOO} = \frac{1}{n} \sum_{i=1}^{n} l(y_i, f(x_i | \mathcal{D} \setminus \mathcal{D}_b)).$$

Note that LOO-CV actually performs a complete $n$-fold CV. However, since the model has to be trained $n$ times, LOO-CV is computationally demanding. On the other hand, it leads to an almost unbiased estimate of the generalization error, but at the expense of an increased variance of the estimator. In general, cross-validation schemes provide a nearly unbiased estimate of the generalization error, at the cost of significant variability, particularly for discontinuous loss functions Efron and Tibshirani (1993). In order to achieve a good compromise between bias and variance the use of 10-fold or 5-fold CV are often recommended.

4.1.2. Bootstrapping

In case of discontinuous error functions bootstrap methods Efron and Tibshirani (1993) may smooth over possible discontinuity. A bootstrap sample $\mathcal{b}$ is created by sampling $n$ instances with replacement from the original sample $\mathcal{D}$. The bootstrap sample $\mathcal{b}$ is then used for training, while the set left out that is $\mathcal{D} \setminus \mathcal{b}$ serves as validation set. Using a sampling procedure with replacement, the expected size of the validation set is $n(1 - \frac{1}{B})^n \approx 0.368n$. Correspondingly, the training set, which is of size $n$, has $\approx 0.632n$ unique observations which leads to an overestimation of the prediction error. The .632 bootstrap estimator Efron and Tibshirani (1993) corrects for this, by adding the underestimated resubstitution error,

$$\text{err}_{\text{boot}} = \frac{1}{B} \sum_{b} 0.632 \cdot \sum_{i \in b} l(y_i, f(x_i | \mathcal{D})) + 0.368 \cdot \sum_{i=1}^{n} l(y_i, f(x_i | \mathcal{D})).$$

However, the standard bootstrap estimate is an upwardly biased estimator of the model accuracy. In particular, it can become to overly optimistic for excessively complex models that are capable to highly overfit the data.

In the context of a feature subset selection experiment for regression, a comprehensive comparison of different schemes for estimating the generalization error has been conducted in Breiman and Spector (1992). Among others schemes, they compared leave-one-out cross-validation, $K$-fold cross-validation for various $K$, stratified version of cross-validation and bias corrected bootstrap on artificially generated data. For the task of model selection they concluded ten-fold cross-validation to outperform the other methods.

5. Practical Hints for Model Evaluation

5.1. Models with Hyperparameters

Many preprocessing and classification methods have one or more hyperparameters that need to be adjusted to the data by means of model selection. Examples are the kernel width of an Gaussian kernel, the regularization parameter $\lambda$ of the regularized LDA, but also the number of neighbors in a $k$-nearest neighbor approach, or the number of principal components to be selected. According to the previously introduced general concept of model selection, those hyperparameters have to be selected by means of an unbiased estimate of the generalization performance, i.e., have to be evaluated on a validation set that is independent of data used for training. Since the selection of the hyperparameter is an integral part of the model, the model selection scheme and therefore the estimation of the validation error becomes part of the model itself. Consequently, the cross-validation
error that has been used for adjusting the hyperparameter of a model becomes a biased estimate of the overall model performance, as it has been minimized by the model selection. Consequently, to estimate the generalization error of the entire model (including the hyperparameter selection) another independent data set is required.

To emphasize the severity of this issue, let us consider the following illustrative example. Given a fixed data set the classification performance of linear discriminant analysis (without hyperparameters) needs to be compared with the performance of an SVM with a Gaussian kernel. Cross-validation is performed for LDA and also for an SVM using a Gaussian kernel for various combinations of the hyperparameters, i.e., the kernel width and the regularization parameter. One can expect the SVM to yield better results than LDA for some combinations, while it will perform worse for others. Nevertheless, it cannot be concluded that the SVM with the ‘optimal selection’ of its hyperparameters outperforms the LDA solution. Obviously, as it has been minimized by the model selection procedure, the CV-error of the selected SVM is to optimistic about the model performance. Note that the CV-error is a random number that exhibits a certain degree of variability. Accordingly, repeated sampling from the distribution of the CV error will favor models with a larger set of parameter combinations (here, the SVM model). In particular, the smaller CV error for some parameter combinations of the SVM could just be a lucky coincidence induced by repeatedly evaluating the SVM model. The severity of biasing the results depends on several factors, e.g., how much complexity can be controlled by the parameters, dimensionality of the features, and the methods of selecting the parameters.

**Nested Cross-Validation:** In order to obtain an unbiased estimate of the generalization performance of the complete model (including selection of the hyperparameter), an additional data set is required which is independent from both, the training and the validation data. To this end, a nested cross-validation scheme is most appropriate. Algorithmically, it can be described as two nested loops of cross-validation. In the inner loop, the hyperparameter as part of the model has to be selected according to inner CV error, while in the outer loop, the selected models are evaluated with respect to their generalization ability on an independent validation set. The outer loop CV-error is similar to (4.21)

\[
err_{CV} = \frac{1}{n} \sum_{i=1}^{K} \sum_{i \in D_h} l(y_i, f_{CV}(x_i | D^i)).
\]

Here, \(D_h\) denotes the \(k\)th validation set of the outer CV-loop, while we use the short hand notation \(D^i_k\) for the corresponding outer loop training set \(D \setminus D_h\). However, the main difference in the above equation compared to the ordinary \(K\)-fold CV is that the model \(f_{CV}(|D^i|)\) refers to the model that has been selected via the inner \(K\)-fold CV over the data set \(D^i\), i.e.,

\[
f_{CV}(|D^i|) := \underset{f \in \mathcal{F}}{\arg\min} \frac{1}{|D^i|} \sum_{i \in D^i} l(y_i, f(x_i | D^i \setminus D^i_k)).
\]

with \(\mathcal{F}\) denoting the set of models corresponding to different value of the hyperparameter and \(D^i_k\) denoting the \(i\)th validation set of the inner CV loop. In order to distinguish more easily between the different layers of cross-validation, one often refers to the holdout set \(D_h\) of the outer loop as test sets. Note, in each round of the outer CV loop the model \(f_{CV}(|D^i|)\) and hence the hyperparameter that is selected can be different. Consequently, nested CV will provide a probability distribution how often a hyperparameter had been selected by the model selection scheme rather than a particular value. On the other hand nested CV gives an unbiased estimate of the generalization performance of the complete model (including selection of the hyperparameters).

### 5.2. Cross-Validation for Dependent Data

Another practical issue when estimating the generalization error of a model is the validity of the assumption about the independence of the training and the validation data. Obviously, if all instances are distributed independently and identically then arbitrary splits into training and validation set will yield stochastically independent samples and the prerequisite is trivially fulfilled. However, often the experimental design induces dependencies between samples. In such a case, special care is required when splitting the sample in order to ensure the aforementioned independence assumption.

For example, a frequently used paradigm in human brain research divides the course of an experiment into blocks of different experimental conditions. We say that an experiment has a block design, if each block comprises several single-trials all belonging to the same condition, see Fig. 8-a.

In such a setting, special care has to be taken in validating the classification of single-trials according to the experimental conditions. Typically, samples within such a block are likely to be stochastically dependent, while stochastic independence can be generally assumed for samples belonging to different blocks. To
Figure 8: Schema of a block design experiment. (a) Alternation between the two conditions that are to be discriminated is on a longer time scale, compared to shorter segments for which classification is evaluated. This setting requires special treatment for validation. (b) Applying cross validation on the epochs violates the assumption that samples in the training set are independent from the ones in the test set. Due to slowly changing nonstationarities in the brain signals, a trial in the test set is very likely to be classified correctly, if trials from the same block are in the training set.

illustrate this, let us consider a neuroimaging recording. Here, typically many slowly varying processes of background activity exist, and hence neighboring trials within a single block are dependent with respect to the information they share about the state of these slow cortical processes. Consequently, applying a simple hold-out strategies as they are conventionally employed by generic LOO or K-fold CV, to block design data will most likely violate the assumption of independence between the training and validation data, see Fig. 8-b.

In order to demonstrate the possible effect of applying a standard CV scheme to block-wise data, we will conduct an illustrative experiment to demonstrate the failure of a generic CV, that severely underestimates the generalization performance. Moreover, we show that the block CV scheme introduced below yields an accurate estimate of the generalization error. However, before we present this example, we will formally introduce a cross-validation scheme that is tailored to the particular needs of block-wise data.

5.2.1. Block Cross-validation

As indicated, data within a single block are likely to be stochastically dependent, while stochastic independence can be assumed for data across blocks. Consequently, the most simple form of a cross-validation scheme for block-wise data corresponds to a leave-one-block-out cross-validation. Analog to LOO-CV a single block is left out for validation and the model is trained on the remaining data. For most of the experimental paradigms such a CV scheme will be appropriate.

However, in order to introduce a more general block-wise CV method, we will assume that for some pre-defined constant \( h \in \mathbb{N} \) the covariance matrices \( \text{Cov}(\{x_i, y_i\}, \{x_{i+j}, y_{i+j}\}) \) (measured in a suitable norm) are of negligible magnitude for all \( |j| > h \). That is, samples that are further apart than \( h \) samples are assumed to be uncorrelated. A so-called \( h \)-block cross-validation scheme is a modification of the LOO-CV scheme. Similar to LOO-CV it uses each instance \((x_i, y_i)\) once as validation set, but unlike LOO-CV it leaves an \( h \)-block (of size \( 2h + 1 \)) of the neighboring \( h \) samples from each side of the \( i \)-th sample out of the training set. Following the notation in Racine (2000), we denote the \( h \)-block by \((x_{(hi)}, y_{(hi)})\), thus the training set of the \( i \)-th iteration corresponds to \( D_{(i \setminus h)} := D \setminus \{x_{(hi)}, y_{(hi)}\} \). The generalization error of the model is consequently obtained by the cross validation function

\[
(5.26) \quad \text{err}_h = \frac{1}{n} \sum_{j=1}^{n} \langle y_j, f(x_j | D_{(i \setminus h)}) \rangle.
\]

Although the latter policy resolves the problem of dependencies, it still has one major drawback. As it was shown in Shao (1993) for the particular choice of the mean squared error as loss function, due to the small size of the validation sets the \( h \)-block cross-validation is inconsistent for the important model class of linear functions. This means, even asymptotically (i.e., for \( n \to \infty \) \( h \)-block cross-validation does not reliably select the true model \( f^* \) from a class of linear models.

As worked out in Racine (2000), a way out of this pitfall is a technique called \( hv \)-cross validation. Heuristically spoken, \( hv \)-cross validation enlarges the validation sets sufficiently. To this end, for a “sufficiently large” \( v \) each validation set is expanded by \( v \) additional observations from either side, yielding \( D_i = (x_{vi}, y_{vi}) \). Hence, each validation set \( D_i \) is of size \( n_i = 2v + 1 \). Moreover, in order to take care of the dependencies, \( h \) observations on either side of \((x_{(vi)}, y_{(vi)})\) are additionally removed to form the training data. Hence, the training data of the \( i \)-th iteration is \( D_{(i \setminus (h + v))} := D \setminus \{x_{(vi)}, y_{(vi)}\} \). Now, the cross-validation function

\[
(5.27) \quad \text{err}_{hv} = \frac{1}{n_i(n - 2v)} \sum_{i=1}^{n} \sum_{j \in D_i} ||y_j - f(x_j | D_{(i \setminus (h + v))})||^2
\]

is an appropriate measure of the generalization error. For asymptotic consistency it is necessary that \( \lim_{h \to \infty} n_i/n = 1 \), thus choosing \( v \) such that \( v = (n - n^h - 2h - 1)/2 \) for a constant \( 0 < \delta < 1 \) is sufficient to achieve consistency (Shao (1993)).

5.3. Caveats in Applying Cross-Validation

Preprocessing the data prior to the application of cross-validation also requires particular care to avoid bi-
as the generalization error of the model. Here, in order to adhere to the independence assumption of training and validation set, any parameters of the preprocessing needs to be estimated solely on the training set and not on the test set. This holds likewise for the estimation of principle and independent component analysis, but also for simpler preprocessing strategies, such as normalization of the data. If cross-validation is used, the estimation of the parameters of preprocessing has to be performed within the cross-validation loop on each training set separately and afterwards transfer to the corresponding test and validation data, respectively. In order to achieve a stringently sound validation, it is for example inappropriate to perform ICA on the entire data, select desirable components and use features extracted from those components as input to a classifier, whose performance needs to be evaluated by cross-validation. Although the bias induced by unsupervised preprocessing techniques will usually be not as severe, it can result in improper model selection and overoptimistic results. In contrast, strong overfitting may occur, if a preprocessing method which uses class label information is performed on the whole data set.

5.4. Model Evaluation Allowing for Feature Selection

Feature selection is widely used in order to decrease the dimensionality of the feature vectors and thus to facilitate classification. Typically, feature selection methods are supervised, i.e., they exploit the label information of the data. A simple strategy is, e.g., to select those features that have a large separability index like Fisher Score (Müller et al. (2004)). A more sophisticated strategy is to use classifiers for feature selection, as, e.g., in Müller et al. (2004); Lal et al. (2004); Blankertz et al. (2006a); Tomioka and Müller (2010). For the same reasons as laid out in Section 5.3 it is vital for a sound validation that such feature selection methods are not performed on the whole data. Again, cross-validation has to be used to evaluate the entire model including feature selection scheme, rather then just cross validating the final step of classification. More specifically, feature selection has to be performed within the cross-validation loop on each training set.

5.5. Model Evaluation Allowing for Outlier Rejection

It requires a prudent approach to fairly evaluate the performance of models which employ outlier rejection schemes. While the rejection of outliers from the training data set is unproblematic, their exclusion from the test set is rather not. Here, two issues have to be considered. (1) The rejection criterion must not use the labels of the test data, and all parameters (such as thresholds) have to be estimated on the training data. (2) For evaluation, a metric has to be used, that takes into account the rejection of trials. Obviously, the rejection of test samples in a classification task means a reduced amount of information compared to a method that obtains the same classification accuracy on all test samples. See Ferrez and Millán (2005) for an application of a performance measure based on Shannon’s information theory in the context of rejected samples based on the detection of an error-related brain response.

An outlier rejection method may use label information (e.g., when class-conditional Mahalanobis distances are used), but only training data may be used to determine parameters of the method, as in the estimation of the covariance matrix for the Mahalanobis distance.

5.6. Loss Functions Allowing for Unbalanced Classes

The classification performance is always evaluated by some loss function, see Section 4.1. Typical examples are 0-1-loss (i.e., average number of misclassified samples) and area under the receiver operator characteristic (ROC) curve (Fawcett (2006)). When using misclassification rate, it must be assured that the classes have approximately the same number of samples. Otherwise, a performance measure that respects the sizes of the classes (or the priors one has about their frequency in the application case) has to be employed. In odd-ball paradigms, e.g., the task is to discriminate brain responses to an attended rare stimulus from responses to a frequent stimulus, a typical ratio of frequent-to-rare stimuli is 85:15. In such a setting, an uninformative classifier which always predicts the majority class would obtain an accuracy of 85%. Accordingly, a different loss functions needs to be employed. Denoting the number of samples in class $i$ by $n_i$, the normalized error can be calculated as weighted average, where errors committed on samples of class $i$ are weighted by $n_i/N$.

5.7. Regarding Nonstationarities

It is worth to note that any cross-validation scheme implicitly relies on the assumption that the samples are identically distributed. In the context of neurophysiological data this transfers to an assumption of stationarity. Unfortunately, nonstationarities are ubiquitous in neuroimaging data (e.g. Shenoy et al. (2006)). Accordingly, the characteristics of brain signals and, in particular, the feature distributions, often change slowly with time. Therefore, a model fitted to data from the beginning of an experiment may not generalize well on
data towards the end of the experiment. This detrimental effect is obscured, when estimating the generalization performance by cross validation, since training samples are drawn from the full time course of the experiment. Accordingly, the classifier is, so to say, prepared for the nonstationarities that occur within the data. Therefore, it is advisable to compare the results of cross-validation with a so called chronological validation, in which the (chronologically) first half of the data is used for training and the second half for testing. If the data includes nonstationarities and the classifier fails to be invariant against them, the chronological validation would predict a substantially worse performance than cross-validation. This situation indicates that the method will suffer from nonstationarity during online operation. In general, one can avoid non-stationarity by (a) constructing invariant features (e.g. Blankertz et al. (2008a)), (b) tracking nonstationarity (e.g. Schlögl et al. (2009); Vidaurre and Blankertz (2010); Vidaurre et al. (2010)), (c) modeling nonstationarity and adapting CV schemes (Sugiyama et al. (2007)), or by (d) projecting to stationary subspaces (von Bünau et al. (2009)).

6. Conclusion

Decoding brain states is a difficult data analytic endeavor, e.g., due to the unfavorable signal to noise ratio, the vast dimensionality of the data, the high trial-to-trial variability etc. In the past, machine learning and pattern recognition have provided significant contributions to alleviate these issues and thus have had their share in many of the recent exciting developments in the neurosciences. In this work, we have introduced some of the most common algorithmic concepts, first from a theoretical viewpoint and then from a practical neuroscience data analyst's perspective. Our main original contribution in this review is a clear account for the typical pitfalls, see Table 1.

Due to space constraints, the level of mathematical sophistication and the number of algorithms described are limited. However, a detailed account was given for the problems of hyper-parameter choice and model selection, where a proper cross-validation procedure is essential for obtaining realistic results that maintain their validity out-of-sample. Moreover, it should be highly emphasized that the proper inclusion of physiological a-priori knowledge is helpful as it can provide the learning machines with representations that are more useful for prediction than if operating on raw data itself. We consider such a close interdisciplinary interaction between paradigm and computational model as essential.

<table>
<thead>
<tr>
<th>Potential pitfall</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preprocessing the data based on global statistics of the entire data (e.g., normalization using the global mean and variance)</td>
<td>Section 5.3</td>
</tr>
<tr>
<td>Global rejection of artifacts or outliers prior to the analysis (resulting in a simplified test set)</td>
<td>Section 5.5</td>
</tr>
<tr>
<td>Global extraction or selection of features (illegitimate use of information about the test data)</td>
<td>Section 5.4</td>
</tr>
<tr>
<td>Simultaneously selecting model parameters and estimating the model performance by cross validation on the same data (yielding a too optimistic estimate of the generalization error)</td>
<td>Section 5.1</td>
</tr>
<tr>
<td>Insufficient model evaluation for paradigms with block design</td>
<td>Section 5.2</td>
</tr>
<tr>
<td>Neglecting unbalanced class frequencies</td>
<td>Section 5.6</td>
</tr>
<tr>
<td>Disregarding effects of non-stationarity</td>
<td>Section 5.7</td>
</tr>
</tbody>
</table>

Table 1: Hall of Pitfalls. The table presents a (incomplete) list of the most prominent sources of error that one need to take into consideration, when applying machine learning methods to brain imaging data.
We would like to end by adding the remark that an unforeseen progress in algorithmic development has been caused by the availability of high quality data with a clear task description. This has allowed a number of interested non-(computational) neuroscientists to study experimental data even without access to expensive measurement technology Sajda et al. (2003); Blankertz et al. (2004, 2006b). The authors express their hope that this development will extend also beyond EEG data.

Acknowledgement

We would like to thank our former co-authors for allowing us to use prior published material in this review. The studies were partly supported by the Bundesministerium für Bildung und Forschung (BMBF), Fkz 01IB001A/B, 01GQ0850, by the German Science Foundation (DFG, contract MU 987/3-2), by the European Union under the PASCAL2 Network of Excellence, ICT-216886. This publication only reflects the authors’ views. Funding agencies are not liable for any use that may be made of the information contained herein.

Author contributions

SL and KRM produced the draft for the part on the machine learning methods and SL work it out in detail and particularly elaborated on the mathematical foundations of model selection and cross-validation. BB contributed the part on pitfalls in model evaluation. TD contributed the part on cross-validation for dependent data. All authors read and approved the manuscript.


