Covariance Kernels from Bayesian Generative Models

Matthias Seeger
Institute for Adaptive and Neural Computation
University of Edinburgh
5 Forrest Hill, Edinburgh EH1 2QL
seeger@dai.ed.ac.uk

Abstract

We propose the framework of mutual information kernels for learning covariance kernels, as used in Support Vector machines and Gaussian process classifiers, from unlabeled task data using Bayesian techniques. We describe an implementation of this framework which uses variational Bayesian mixtures of factor analyzers in order to attack classification problems in high-dimensional spaces where labeled data is sparse, but unlabeled data is abundant.

1 Introduction

Kernel machines, such as Support Vector machines or Gaussian processes, are powerful and frequently used tools for solving statistical learning problems. They are based on the use of a kernel function which encodes task prior knowledge in a Bayesian manner. In this paper, we propose the framework of mutual information (MI) kernels for learning covariance kernels from unlabeled task data using Bayesian techniques. This section introduces terms and concepts. We also discuss some general ideas for discriminative semi-supervised learning and kernel design in this context. In section 2, we define the general framework and give examples. We note that the Fisher kernel [4] is a special case of a MI kernel. MI kernels for mixture models are discussed in detail. In section 3, we describe an implementation for a MI kernel for variational Bayesian mixtures of factor analyzers and show results of preliminary experiments.

In the semi-supervised classification problem, a labeled dataset $D_l = \{(x_1, t_1), \ldots, (x_m, t_m)\}$ as well as an unlabeled set $D_u = \{x_{m+1}, \ldots, x_{m+n}\}$ are given for training, both i.i.d. drawn from the same unknown distribution, but the labels for $D_u$ cannot be observed. Here, $x_i \in \mathbb{R}^p$ and $t_i \in \{-1, +1\}$. Typically, $m = |D_l|$ is rather small, and $n = |D_u| \gg m$. Our aim is to fit models to $D_u$ in a Bayesian way, thereby extracting (posterior) information, then use this information to build a covariance kernel $K$. Afterwards, $K$ will be plugged into a supervised kernel machine, which is trained on the labeled data $D_l$ to perform the classification task.

1For simplicity, we only discuss binary labels here.
It is important to distinguish very clearly between these two learning scenarios. For fitting \(D_u\), we use Bayesian density estimation. After having chosen a model family \(\{P(x|\theta)\}\) and a prior distribution \(P(\theta)\) over parameters \(\theta\), the posterior distribution \(P(\theta|D_u) \propto P(D_u|\theta)P(\theta)\), where \(P(D_u|\theta) = \prod_{i=m+1}^{n} P(x_i|\theta)\), encodes all information that \(D_u\) contains about the latent (i.e. unobserved) parameters \(\theta\).2

The other learning scenario is supervised classification, using a kernel machine. Such architectures model a smooth latent function \(y(x) \in \mathbb{R}\) as a random process, together with a classification noise model \(P(t|y)\).3 The covariance kernel \(K\) specifies the prior distribution for this process: namely, a-priori, \(y(x)\) is assumed to be a Gaussian process with zero mean and covariance function \(K\), i.e. \(K(x^{(1)},x^{(2)}) = E[y(x^{(1)})y(x^{(2)})]\); see e.g. [10] for details. In the following, we use the notation \(a = (a_1,a_2,a_3,...,a_l)^t\) for vectors, and \(A = (a_{i,j})_{l \times l}\) for matrices respectively. The prime denotes transposition. \(\text{diag}\ a\) is the matrix with diagonal \(a\) and 0 elsewhere. \(N(x|\mu,\Sigma)\) denotes the Gaussian density with mean \(\mu\) and covariance matrix \(\Sigma\).

Within the standard discriminative Bayesian classification scenario, unlabeled data cannot be used. However, it is rather straightforward to modify this scenario by introducing the concept of conditional priors (see [6]). If we have a discriminant model family \(\{P(t|x;w)\}\), a conditional prior \(P(w|\theta)\) allows to encode prior knowledge and assumptions about how information about \(P(x)\) (i.e. about \(\theta\)) influences our assumptions about a-priori probabilities over discriminants \(w\). For example, the \(P(w|\theta)\) could be Occam priors, expressing the intuitive fact that for many problems, the notion of “simplicity” of a discriminant function depends strongly on what is known about the input distribution \(P(x)\). For a given problem, it is in general not easy to come up with a useful conditional prior. However, once such a prior is specified, we can in principle use the same powerful techniques for approximate Bayesian inference that have been developed for supervised discriminative settings. Semi-supervised techniques that can be seen as employing conditional priors include co-training [1], feature selection based on clustering [7] and the Fisher kernel [4]. For a probabilistic kernel technique, \(P(w|\theta)\) is fully specified by a covariance function \(K(x^{(1)},x^{(2)}|\theta)\) depending on \(\theta\). The problem is therefore to find covariance kernels which (as GP priors) favour discriminants in some sense compatible with what we have learned about the input distribution \(P(x)\).

Kernel techniques can be seen as nonparametric smoothers, based on the (prior) assumption that if two input points are “similar” (e.g. “close” under some distance), their labels (and latent outputs \(y\)) should be highly correlated. Thus, one generic way of learning kernels from unlabeled data is to learn a distance between input points from the information about \(P(x)\). A frequently used assumption about how classification labels may depend on \(P(x)\) is the cluster hypothesis: we assume discriminants whose decision boundaries lie between clusters in \(P(x)\) to be a-priori more likely than such that label clusters inconsistently. A general way of encoding this hypothesis is to learn a distance from \(P(x)\) which is consistent with clusters in \(P(x)\), i.e. points within the same cluster are closer under this distance than points from different clusters. We can then try to embed the learned distance \(d(x^{(1)},x^{(2)})\) approximately in an Euclidean space, i.e. learn a mapping \(\phi: x \mapsto \phi(x) \in \mathbb{R}^d\) such that \(d(x^{(1)},x^{(2)}) \approx ||\phi(x^{(1)}) - \phi(x^{(2)})||\) for all pairs from \(D_u\). Then, a natural kernel function would be \(K(x^{(1)},x^{(2)}) = \exp(-\beta ||\phi(x^{(1)}) - \phi(x^{(2)})||^2)\). In this paper, however, we follow a simpler approach, by considering a similarity measure

\(^2\)In practice, computation of \(P(\theta|D_u)\) is hardly ever feasible, but powerful approximation techniques can be used.

\(^3\)A natural choice for binary classification is to represent the log odds \(\log(P(t = +1|x)/P(t = -1|x))\) by \(y(x)\).
which immediately gives rise to a covariance kernel, without having to compute an approximate Euclidean embedding.

**Remark:** Our main aim in this paper is to construct kernels that can be learned from unlabeled data only. In contrast to this, the task of learning a kernel from labeled data is somewhat simpler and can be approached in the following generic way: start with a parametric model family \( \{ y(x; w) \} \), with the interpretation that \( y(x; w) \) models the log odds \( \log(P(t = +1|x)/P(t = -1|x)) \). Fitting these models to labeled data \( D_t \), we obtain a posterior \( P(w|D_t) \). Now, a natural covariance kernel for our problem is simply \( K(x^{(1)}, x^{(2)}) = \int y(x^{(1)}; w)y(x^{(2)}; w)Q(w)dw \), where \( Q(w) \propto P(w|D_t)^\lambda P(w)^{1-\lambda} \) (or an approximation thereof). For \( \lambda = 0 \), we obtain the prior covariance kernel for our model, while for larger \( \lambda \) the kernel incorporates more and more posterior information. The kernel proposed in [8] can be seen as an approximation to this approach.

### 2 Mutual Information Kernels

In this section, we begin by introducing the framework of mutual information kernels. Given a mediator distribution \( P_{med}(\theta) \) over parameters \( \theta \), we define the joint distribution \( Q(x^{(1)}, x^{(2)}) \) mediated by \( P_{med}(\theta) \) as

\[
Q(x^{(1)}, x^{(2)}) = \int P_{med}(\theta)P(x^{(1)}|\theta)P(x^{(2)}|\theta) \, d\theta.
\]

The sample mutual information between \( x^{(1)} \) and \( x^{(2)} \) under this distribution is

\[
I(x^{(1)}, x^{(2)}) = \log \frac{Q(x^{(1)}, x^{(2)})}{Q(x^{(1)})Q(x^{(2)})},
\]

where \( Q(x) = \int Q(x, \tilde{x}) \, d\tilde{x} \). \( I(x^{(1)}, x^{(2)}) \) is called the mutual information (MI) score. In a very concrete sense, it measures the similarity between \( x^{(1)} \) and \( x^{(2)} \) with respect to the generative process represented by the mediator distribution \( P_{med}(\theta) \): it is the amount of information they share via the mediator variable \( \theta \sim P_{med}(\theta) \). Note that \( Q(x^{(1)}, x^{(2)}) \) can be seen as an inner product in a space of functions \( f: \mathbb{R} \rightarrow \mathbb{R} \), the features of \( x^{(k)} \) being \( (P(x^{(k)}|\theta))_\theta \), weighted by the distribution \( P_{med} \). \( x^{(k)} \) is represented by its likelihood under all possible models.

Covariance kernels have to satisfy the property of positive definiteness, and the MI score \( I \) does not. However, applying a standard transformation (called exponential embedding (EE) here), we arrive at

\[
K(x^{(1)}, x^{(2)}) = e^{-\frac{1}{2}I(x^{(1)}, x^{(2)}) + \frac{1}{2}I(x^{(1)}, x^{(1)}) + \frac{1}{2}I(x^{(2)}, x^{(2)})} = \frac{Q(x^{(1)}, x^{(2)})}{\sqrt{Q(x^{(1)}, x^{(1)})Q(x^{(2)}, x^{(2)})}}.
\]

EE becomes familiar if we note that it transforms the standard inner product \( x^{(1)}'x^{(2)} \) into the well-known Radial Basis Function (RBF) kernel

\[
K_{RBF}(x^{(1)}, x^{(2)}) = e^{-\frac{1}{2\beta}\|x^{(1)}-x^{(2)}\|^2},
\]

\( \beta > 0 \) (see e.g. [3]).
or the weighted inner product $x^{(1)'}Dx^{(2)}$ into the squared-exponential kernel (e.g. [10]). It is easy to show that $K$ in (3) is a valid covariance kernel\(^7\), and we refer to it as mutual information (MI) kernel.

**Example:** Let $P(x|\theta) = N(x|\theta,(\rho/2)I)$ (spherical Gaussian with mean $\theta$), $P_{med}(\theta) = N(\theta|\theta,\alpha I)$. Then, the MI kernel $K$ is the RBF kernel (4) with $\beta = 4/(\rho(4+\rho/\alpha))$. Thus, the RBF kernel is a special case of a MI kernel.

### 2.1 Mediator distribution. Model-trust scaling.

The mediator distribution $P_{med}(\theta)$, motivated earlier in this section, should ideally encode information about the $x$ generation process, just as the Bayesian posterior $P(\theta|D_u)$. On the other hand, we need to be able to control the influence that information from sources such as unlabeled data $D_u$ can have on the kernel (relying too much on such sources results in lack of robustness, see e.g. [6] for details). Here, we propose model-trust scaling (MTS), by setting

$$P_{med}(\theta|\lambda) \propto P(D_u|\theta)^{\lambda/n}P(\theta), \quad \lambda \in [0,n]. \quad (5)$$

$P_{med}$ varies with $\lambda$ from the (usually vague) prior $P(\theta)$ ($\lambda = 0$) towards the sharp posterior $P(\theta|D_u)$ ($\lambda = n$), rendering the $D_u$ information (via the model) more and more influence upon the kernel $K$. The concrete effect of MTS on the kernel depends on the model family.

**Example (continued):** Again, $P(x|\theta) = N(x|\theta,(\rho/2)I)$, with a flat prior $P(\theta) = 1$ on the mean. Then, $P(\theta|D_u) = N(\theta|x, (\rho/2n)I)$, where $\hat{x} = n^{-1}\sum_{i=m+1}^{m+n} x_i$, and $P_{med}(\theta) = N(\theta|\hat{x}, (\rho/2\lambda)I)$ (after (5)). Thus, the MI kernel is again the RBF kernel (4) with $\beta = 2/(\rho(2+\lambda))$. For the more flexible model $P(x|\theta) = N(x|\mu, \Sigma)$, $\theta = (\mu, \Sigma)$ and the conjugate Jeffreys prior, the MI kernel is computed in [5].

If the Bayesian analysis is done with conjugate prior-model pairs, the corresponding MI kernel can be computed easily, and for many of these cases, MTS has a very simple, analytic form (see [5]). In general, approximation techniques developed for Bayesian analysis have to be applied. For example, applying the Laplace approximation to the computations on a model with flat prior $P(\theta) = 1$ results in the Fisher kernel [4]\(^8\), see e.g. [5]. However, in this paper we favour another approximation technique (see section 3).

### 2.2 Mutual Information Kernels for Mixture Models

If we apply the MI kernel framework to mixture models $P(x|\theta, \pi) = \sum_s \pi_s P(x|\theta_s)$, we run into a problem. As mentioned in section 1, we would like our kernel at least partly to encode the cluster hypothesis, i.e. $K(x^{(1)}, x^{(2)})$ should be small if $x^{(1)}$, $x^{(2)}$ come from different clusters in $P(x)$,\(^9\) but the opposite is true (for not too small

\(^7\) $Q(x^{(1)}, x^{(2)})$ is an inner product (therefore a kernel), for the rest of the argument see [3], section 5.

\(^8\) This was essentially observed by the authors of [4] on workshop talks, but has not been published to our knowledge. The fascinating idea of the Fisher kernel has indeed been the main motivation and inspiration for this paper.

\(^9\) This does not mean that we (a-priori) believe they should have different labels, but only that the label (or better: the latent $y(\cdot)$) at one of them should not depend strongly on $y(\cdot)$ at the other.
To overcome this problem, we generalize $Q(x^{(1)}, x^{(2)})$:

$$Q(x^{(1)}, x^{(2)}) = \sum_{s_1, s_2 = 1}^{S} w_{s_1, s_2} \int P(x^{(1)} | \theta_{s_1}) P(x^{(2)} | \theta_{s_2}) P_{med}(\theta) d\theta,$$

where $W = (w_{s_1, s_2})_{s_1, s_2}$ is symmetric with nonnegative entries and positive elements on the diagonal. The MI kernel $K$ is defined as before by (3), based on the new $Q$. If $P_{med}(\theta, \pi) = \prod_{s} P_{med}(\theta) P_{med}(\pi)$ (which is true for the cases we will be interested in), we see that the original MI kernel arises as special case $w_{s_1, s_2} = E_{P_{med}(\pi_{s_1, s_2})}$. Now, by choosing $W = \text{diag}(E_{P_{med}(\pi_{s})})$, we arrive at a MI kernel $K$ which (typically) behaves as expected w.r.t. cluster separation (see figure 1), but does not exhibit long-range correlations between joined components. In the present work, we restrict ourselves to this diagonal mixture kernel. Note that this kernel can be seen as (normalized) mixture of MI kernels over the component models.

![Figure 1: Kernel contours on 2-cluster dataset ($\lambda = 5, 100, 30$)](image)

Figure 1 shows contour plots of the diagonal mixture kernel for VB-MoFA (see section 3), learned on a 500 cases dataset sampled from two Gaussians with equal covariance (see subsection 3.1). We plot $K(\mathbf{a}, \mathbf{x})$ for fixed $\mathbf{a}$ (marked by a cross) against all $\mathbf{x}$, the height between contour lines is $0.1$. The left and middle plot have the lower cluster's centre as $\mathbf{a}$, with $\lambda = 5$, $\lambda = 100$ respectively, the right plot's $\mathbf{a}$ lies between the cluster centres, $\lambda = 30$. The effect of MTS can be seen by comparing left and middle, note the different sharpness of the slopes towards the other cluster and the different sizes and shapes of the “high correlation” regions. As seen on the right, points between clusters have highest correlation with other such inter-cluster points, a feature that may be very useful for successful discrimination.

### 3 Experiments with Mixtures of Factor Analyzers

In this section, we describe an implementation of a MI kernel, using variational Bayesian mixtures of factor analyzers (VB-MoFA) [2] as density models. These are able to combine local dimensionality reduction (using noisy linear transformations $\mathbf{u} \rightarrow \mathbf{x}$ from low-dimensional latent spaces) with good global data fit using mixtures. VB-MoFA is a variational approximation to Bayesian analysis on these models, able to deliver the posterior approximations we require for an MI kernel.

We employ the diagonal mixture kernel (see subsection 2.2). Instead of implementing MTS analytically, we compute the VB approximation to the true posterior (i.e. $\lambda = n$), then simply apply the scaling to this distribution. $P_{med}(\theta, \pi)$ factorizes as required in subsection 2.2. The integrals $\int P(x^{(1)} | \theta_{s_1}) P(x^{(2)} | \theta_{s_2}) P_{med}(\theta) d\theta$ in (6)

10Produced using the first-order approximation (see 3) to the MI kernel. Plots using the one-step variational approximation (see 3) have a somewhat richer structure.
are not analytically tractable. Our first idea was to approximate them by applying the VB technique once more, ending up with what we called one-step variational approximations. Unfortunately, the MI kernel approximation based on these terms cannot be shown to be positive definite anymore\footnote{Thanks to an anonymous reviewer for pointing out this flaw.}. Thus, in the moment we use a less elegant and, we feel, less accurate approximation (details can be found in [5]) based on first-order Taylor expansions.

In the remainder of this section we compare the VB-MoFA kernel with the RBF kernel (4) on two datasets, using a Laplace GP classifier (see [10]). In each case we sample a training pool, a kernel dataset $D_u$ and a test set (mutually exclusive). The VB-MoFA diagonal mixture kernel is learned on $D_u$. For a given training set size $m$, a run consists of sampling a training set $D_t$ and a holdout set $D_h$ (both of size $m$) from the training pool, tuning kernel parameters by validation on $D_h$, then testing on the test set. We use the same $D_t, D_u$ for both kernels. For each training set size, we do $L = 30$ runs. Results are presented by plotting means and 95\% $t$-test confidence intervals of test errors over runs.

### 3.1 Two Gaussian clusters

The dataset is sampled from two 2-d Gaussians with same non-spherical covariance (see figure 1), one for each class (the Bayes error is 2.64\%). We use $n = 500$ points for $D_u$, a training pool of 100 and a test set of 500 points. The learning curves in figure 2 show that on this simple toy problem, on which the fitted VB-MoFA model represents the cluster structure in $P(x)$ almost perfectly, the VB-MoFA MI kernel outperforms the RBF kernel for samples sizes $n \leq 40$.

![Learning curves on 2-cluster dataset. Left: RBF kernel; right: MI kernel](image)

### 3.2 Handwritten Digits (MNIST): Twos against threes

We report results of preliminary experiments using the subset of twos and threes of the MNIST Handwritten Digits database\footnote{The $28 \times 28$ images were downsampled to size $8 \times 8$.}. Here, $n = |D_u| = 2000$, the training pool contains 8089, the test set 2000 cases. We employ a VB-MoFA model with 20 components, fitted to $D_u$. We use a very simple baseline (BL) algorithm (see [6], section 2.3) based on the component densities from the VB-MoFA model\footnote{The estimates $P(x|\theta_s)$ are obtained by integrating out the parameters $\theta_s$ using the variational posterior approximation. The integral is not analytic, and we use a one-step variational approximation to it.}, which
allows us to assess the "purity" of the component clusters w.r.t. the labels\textsuperscript{14}; this algorithm is the only one not based on a kernel. Furthermore, we show results for the one-step variational approximation to the MI kernel\textsuperscript{15} (MIOLD). The learning curves are shown in figure 3.

![Learning curves on MNIST twos/threes. Upper left: RBF kernel; upper middle: Baseline method; upper right: VB-MoFA MI kernel (first-order approx.); lower left: VB-MoFA MI "kernel" (one-step var. approx.)](image)

Figure 3: Learning curves on MNIST twos/threes. Upper left: RBF kernel; upper middle: Baseline method; upper right: VB-MoFA MI kernel (first-order approx.); lower left: VB-MoFA MI "kernel" (one-step var. approx.)

The results are disappointing. The fact that the first-order approximation to the MI kernel performs worse than the one-step variational approximation (although the latter may fail to be positive definite), indicates that the former is a poorer approximation. The latter renders results close to the baseline method, while the smoothing RBF kernel makes much better use of a growing number of labeled examples\textsuperscript{16} This indicates that the conditional prior, as represented by the VB-MoFA MI kernel, behaves nonsmooth and overrides label information in regions where it should not. We suspect this problem to be related to the high dimensionality of the input space, in which case probability densities tend to have a large dynamic range, and mixture component responsibility estimates tend to behave very nonsmooth. Thus, it seems to be necessary to extend the basic MI kernel framework by new scaling mechanisms in order to produce a smoother encoding of the prior assumptions.

\textsuperscript{14}The baseline algorithm is based on the assumption that, given the component index \( s \), the input point \( x \) and the label \( t \) are independent. Only the conditional probabilities \( P(t|s) \) are learned, while \( P(x|s) \) and \( P(s) \) is obtained from the VB-MoFA model fitted to unlabeled data only. Thus, success/failure of this method should be closely related to the degree of purity of the component clusters w.r.t. the labels.

\textsuperscript{15}This is somewhat inconsistent, since we use a kernel function which might not be positive definite in a context (GP classification) which requires a covariance function.

\textsuperscript{16}Note also that RBF kernel matrices can be evaluated significantly faster than such using the VB-MoFA MI kernel.
4 Related work. Discussion

The present work is probably most closely related to the Fisher kernel (see subsection 2.1). The arguments concerning mixture models (see subsection 2.2) apply there as well. Haussler [3] contains a wealth of material about kernel design for discrete objects $x$. Watkins [9] mentions that expressions like $Q$ in (1) are valid kernels for discrete $x$ and countable parameter spaces. Very recently we came across [11], which essentially describes a special case of the diagonal mixture kernel (see subsection 2.2) for Gaussian components with diagonal covariances\footnote{The $\alpha$ parameter in this work is related to MTS in this case.}. The author calls $Q$ a stochastic equivalence predicate. He is interested in distance learning, does not apply his method to kernel machines and does not give a Bayesian interpretation.

We have presented a general framework for kernel learning from unlabeled data and described an approximate implementation using VB-MoFA models. A straightforward application of this technique to high-dimensional real-world data did not prove successful, and in future work we will explore new ideas for extending the basic MI kernel framework in order to be able to deal with high-dimensional input spaces.

Acknowledgments

We thank Chris Williams for many inspiring discussions, furthermore Ralf Herbrich, Amos Storkey, Hugo Zaragoza and Neil Lawrence. Matt Beal helped us a lot with VB-MoFA. The author gratefully acknowledges support through a research studentship from Microsoft Research Ltd.

References