Information Theoretic Model Selection for Pattern Analysis

Joachim M. Buhmann
Morteza Haghir Chehreghani
Mario Frank
Andreas P. Streich

Department of Computer Science, ETH Zurich, Switzerland

Editor: I. Guyon, G. Dror, V. Lemaire, G. Taylor, and D. Silver

Abstract

Exploratory data analysis requires (i) to define a set of patterns hypothesized to exist in the data, (ii) to specify a suitable quantification principle or cost function to rank these patterns and (iii) to validate the inferred patterns. For data clustering, the patterns are object partitionings into $k$ groups; for PCA or truncated SVD, the patterns are orthogonal transformations with projections to a low-dimensional space. We propose an information theoretic principle for model selection and model-order selection. Our principle ranks competing pattern cost functions according to their ability to extract context sensitive information from noisy data with respect to the chosen hypothesis class. Sets of approximative solutions serve as a basis for a communication protocol. Analogous to Buhmann (2010), inferred models maximize the so-called approximation capacity that is the mutual information between coarsened training data patterns and coarsened test data patterns. We demonstrate how to apply our validation framework by the well-known Gaussian mixture model.

Keywords: Unsupervised learning, data clustering, model selection, information theory, maximum entropy, approximation capacity

1. Model Selection via Coding

Model selection and model order selection [Burnham and Anderson (2002)] are fundamental problems in pattern analysis. A variety of models and algorithms has been proposed to extract patterns from data, i.e., for clustering, but a comprehensive theory on how to choose the “right” pattern model given the data is still missing. Statistical learning theory as in Vapnik (1998) advocates to measure the generalization ability of models and to employ the prediction error as a measure of model quality. In particular, stability analysis of clustering solutions has shown very promising results for model order selection in clustering [Dudoit and Fridlyand (2002); Lange et al. (2004)], although discussed controversially by Ben-David et al. (2006). Stability is, however, only one aspect of statistical modeling, e.g., for unsupervised learning. The other aspect of the modeling tradeoff is characterized by the informativeness of the extracted patterns. A tolerable decrease in the stability of inferred patterns in the data (data model) might be compensated by a substantial increase of their information content (see also the discussion in Tishby et al. (1999)).

We formulate a principle that balances these two antagonistic objectives by transforming the model selection problem into a generic communication scenario. Thereby, the objective
function or cost function that maps patterns to quality scores is considered as a noisy channel. Different objectives are ranked according to their transmission properties and the cost function with the highest channel capacity is then selected as the most informative model for a given data set. Thereby, we generalize the set-based coding scheme proposed by Buhmann (2010) in order to simplify the embedding of pattern inference problems in a communication framework. Learning, in general, resembles communication from a conceptual viewpoint: For communication, one demands a high rate (a large amount of information transferred per channel use) together with a decoding rule that is stable under the perturbations of the messages by the noise in the channel. For learning patterns in data, the data analyst favors a rich model with high complexity (e.g., a large number of clusters in grouping), while the generalization error of test patterns is expected to remain stable and low. We require that solutions of pattern analysis problems are reliably inferred from noisy data.

This article first develops the information theoretic framework of weighted approximation set coding (wASC) for validating statistical models. We then demonstrate for the first time, how to practically transform a pattern recognition task to a communication setting and how to compute the capacity of clustering solutions. The feasibility of wASC is demonstrated for mixture models and real world data.

2. Brief Introduction to Approximation Set Coding

In this section, we briefly describe the theory of weighted Approximation Set Coding (wASC) for pattern analysis as proposed by Buhmann (2010).

Let \( X = \{X_1, \ldots, X_n\} \in \mathcal{X} \) be a set of \( n \) objects \( O \) and \( n \) measurements in a data space \( \mathcal{X} \), where the measurements characterize the objects. Throughout the paper, we assume the special case of a bijective map between objects and measurements, i.e., the \( i \)th object is synonymous with the vector \( x_i \in \mathbb{R}^D \). In general, the (object, measurement) relation might be more complex than an object-specific feature vector. A hypothesis, i.e. a solution of a pattern analysis problem, is a function \( c : \mathcal{X} \to P \), \( X \mapsto c(X) \).

Accordingly, the hypothesis class is the set of all such functions, i.e. \( \mathcal{C}(X) := \{c(X) : X \in \mathcal{X}\} \). For clustering, the patterns are object partitionings \( P = \{1, \ldots, k\}^n \). A model for pattern analysis is characterized by a cost/objective function \( R(c, X) \) that assigns a real value to a pattern \( c(X) \). To simplify the notation, model parameters \( \theta \) (e.g., centroids) are not explicitly listed as arguments of the objective function. Let \( c^\perp(X) \) be the pattern that minimizes the cost function, i.e. \( c^\perp(X) := \arg\min_c R(c, X) \). For normalization purposes we assume that the minimal costs \( R(c^\perp, X) = 0 \) vanish. As the measurements \( X \) are random variables, the global minimum \( c^\perp(X) \) of the empirical costs is a random variable as well. Let \( X^{(q)}, q \in \{1, 2\} \), be two datasets with the same inherent structure but different noise instances. In most cases, their global minima differ, i.e. \( c^\perp(X^{(1)}) \neq c^\perp(X^{(2)}) \). In order to rank all solutions of the pattern analysis problem, we introduce approximation weights

\[
w : \mathcal{C} \times \mathcal{X} \times \mathbb{R}_+ \to [0, 1], \quad (c, X, \beta) \mapsto w_\beta(c, X).
\]
Thereby, we require that i) weights should be non-negative and ii) solutions with lower costs should have a larger weight, i.e.,

\[ R(c, X) \leq R(\hat{c}, X) \iff w_\beta(c, X) \geq w_\beta(\hat{c}, X). \]

The family of (Boltzmann) weights \( w_\beta(c, X) := \exp(-\beta R(c, X)) \), parameterized by the inverse computational temperature \( \beta \), fulfils these requirements. These weights define the two weight sums \( Z_q \) and the joint weight sum \( Z_{12} \)

\[
Z_q := Z(X^{(q)}) = \sum_{c \in \mathcal{C}(X^{(q)})} \exp(-\beta R(c, X^{(q)})), \quad q = 1, 2 \tag{4}
\]

\[
Z_{12} := Z(X^{(1)}, X^{(2)}) = \sum_{c \in \mathcal{C}(X^{(2)})} \exp(-\beta(R(c, X^{(1)}) + R(c, X^{(2)}))), \tag{5}
\]

where \( \exp(-\beta(R(c, X^{(1)}) + R(c, X^{(2)}))) \) measures how well a solution \( c \) minimizes costs on both datasets. The sums (4,5) play a central role in our framework. If \( \beta = 0 \), all weights \( w_\beta(c, X) = 1 \) are independent of the costs. In this case, \( Z_q = |\mathcal{C}(X^{(q)})| \) indicates the size of the hypothesis space, and \( Z_{12} = Z_1 = Z_2 \). For high \( \beta \), all weights are small compared to the weight \( w_\beta(c^\perp, X^{(q)}) \) of the global optimum and the weight sum essentially counts the number of globally optimal solutions. For intermediate \( \beta \), \( Z(\cdot) \) takes a value between 0 and \( |\mathcal{C}(X^{(q)})| \), giving rise to the interpretation of \( Z(\cdot) \) as the effective number of patterns that approximately fit the dataset \( X^{(q)} \), where \( \beta \) defines the precision of this approximation. Essentially, \( Z_q \) counts all statistically indistinguishable data patterns that approximate the minimum of the objective function. The global optimum \( c^\perp(X) \) can change whenever we optimize on another random subset of the data, whereas, for a well-tuned \( \beta \), \( Z(X) \) remains approximately invariant. Therefore, \( Z(X) \) defines the resolution of the hypothesis class that is relevant for inference. Noise in the measurements \( X \) reduces this resolution and thus coarsens the hypothesis class. As a consequence, the key problem of learning is to control the resolution optimally: How high can \( \beta \) be chosen to still ensure identifiability of \( Z(X) \) in the presence of data fluctuations? Conversely, choosing \( \beta \) too low yields a too coarse resolution of solutions and does not capture the maximal amount of information in the data.

We answer this key question by means of a communication scenario. The communication architecture includes a sender \( S \) and a receiver \( R \) with a problem generator \( \mathcal{PG} \) between the two terminals \( S, R \) (see Fig. 1). The communication protocol is organized in two stages: (i) design of a communication code and (ii) the communication process.
For the communication code, we adapt Shannon’s random coding scenario, where a codebook of random bit strings covers the space of all bit strings. The sender sends a bit string and the receiver observes a perturbed version of this bit string. For decoding, the receiver has to find the most similar codebook vector in the codebook which is the decoded message. In the same spirit, for our scenario, the sender must communicate patterns to the receiver via noisy datasets. Since we are interested in patterns with low costs, the optimal pattern $c^\perp(X^{(1)})$ can serve as a message. The other patterns in the codebook are generated by transforming the training data $\tau \circ X^{(1)}$ with the transformation $\tau \in \mathbb{T} := \{\tau_1, \ldots, \tau_{2^n\rho}\}$. The number of codewords is $2^{n\rho}$ and $\rho$ is the rate of the protocol. The choice of such transformations depends on the hypothesis class and they have to be equivariant, i.e., the transformed optimal pattern equals the optimal pattern of the transformed data $\tau \circ c(X^{(1)}) = c(\tau \circ X^{(1)})$.

In data clustering, permuting the indices of the objects defines the group of transformations to cover the pattern space. Each clustering solution $c \in C(X^{(1)})$ can be transformed into another solution by a permutation $\tau$ on the indices of $c$. To communicate, $S$ selects a transformation $\tau_s \in \mathbb{T}$ and sends it to a problem generator $PG$ as depicted in Fig. 1. $PG$ then generates a new dataset $X^{(2)}$, applies the transformation $\tau_s$, and sends the resulting data $\tilde{X} := \tau_s \circ X^{(2)}$ to $R$. On the receiver side, the lack of knowledge on the transformation $\tau_s$ is mixed with the stochastic variability of the source generating the data $X$. $R$ has to estimate the transformation $\hat{\tau}$ based on $\tilde{X}$. The decoding rule of $R$ selects the pattern transformation $\hat{\tau}$ that yields the highest joint weight sum of $\hat{\tau} \circ X^{(1)}$ and $\tilde{X}$

$$\hat{\tau} = \arg \max_{\tau \in \mathbb{T}} \sum_{c \in C(X^{(1)})} \exp(-\beta(R(c, \tau \circ X^{(1)}) + R(c, \tilde{X}))). \tag{6}$$

In the absence of noise in the data, we have $X^{(1)} = X^{(2)}$, and error-free communication works even for $\beta \to \infty$. The higher the noise level, the lower we have to choose $\beta$ in order to obtain weight sums that are approximately invariant under the stochastic fluctuations in the measurements thus preventing decoding errors. The error analysis of this protocol investigates the probability of decoding error $\mathbb{P}(\hat{\tau} \neq \tau_s | \tau_s)$. As derived for an equivalent channel in Buhmann (2011), an asymptotically vanishing error rate is achievable for rates

$$\rho \leq I_\beta(\tau_j, \hat{\tau}) = \frac{1}{n} \log \left( \frac{|\{\tau_j\}| Z_{12}}{Z_1Z_2} \right) = \frac{1}{n} \left( \log \frac{|\{\tau_j\}|}{Z_1} + \log \frac{|C^{(2)}|}{Z_2} - \log \frac{|C^{(2)}|}{Z_{12}} \right) \tag{7}$$

The three logarithmic terms in eq.(7) denote the mutual information between the coarsening of the pattern space on the sender side and the coarsening of the pattern space on the receiver side.

The cardinality $|\{\tau_j\}|$ is determined by the number of realizations of the random transformation $\tau$, i.e. by the entropy of the type (in an information theoretic sense) of the empirical minimizer $c^\perp(X)$. As the entropy increases for a large number of patterns, $|\{\tau_j\}|$ accounts for the model complexity or informativeness of the solutions. For noisy data, the communication rate is reduced as otherwise the solutions can not be resolved by the receiver. The relative weights are determined by the term $Z_{12}/(Z_1 \cdot Z_2) \in [0,1]$ which accounts for the stability of the model under noise fluctuations.
In analogy to information theory, we define the approximation capacity as

$$CAP(\tau_n, \hat{\tau}) = \max_\beta I_\beta(\tau_n, \hat{\tau}). \quad (8)$$

Using these entities, we can describe how to apply the wASC principle for model selection from a set of cost functions \( \mathcal{R} \): Randomly split the given dataset \( \mathbf{X} \) into two subsets \( \mathbf{X}^{(1)} \) and \( \mathbf{X}^{(2)} \). For each candidate cost function \( R(c, \mathbf{X}) \in \mathcal{R} \), compute the mutual information (eq. 7) and maximize it with respect to \( \beta \). Then select the cost function that achieves highest capacity at the best resolution \( \beta^* \).

3. Approximation Capacity for Mixture of Gaussians

In this section, we demonstrate the principle of maximum approximation capacity on the well known Gaussian mixture model (GMM). We first derive how to calculate the approximation capacity for GMMs and then we experimentally compare it against other model selection principles.

3.1. Calculation of Approximation Capacity for Gaussian Mixture Models

A GMM with \( K \) components is defined as \( p(\mathbf{x}) = \sum_{k=1}^{K} \pi_k \mathcal{N}(\mathbf{x} | \mathbf{\mu}_k, \mathbf{\Sigma}) \), with non-negative \( \pi_k \) and \( \sum_k \pi_k = 1 \). For didactical reasons, we do not optimize the covariance matrix \( \mathbf{\Sigma} \) and simply fix it to \( \mathbf{\Sigma} = 0.5 \cdot \mathbf{I} \). Then, maximizing the GMM likelihood essentially boils down to centroid-based clustering. As follows, we calculate the approximation capacity in two steps: i) calculate the weight sums \( Z_q, q = 1, 2 \), and the joint weight sum \( Z_{12} \); ii) maximize \( I_\beta \) w.r.t. \( \beta \) (eq. 7).

For calculating the weight sums, we introduce two auxiliary variables. Let \( \mathbf{M} \) be the cluster assignment matrix encoding the clustering solution \( c \). It assigns objects to clusters with \( M_{i,k} \in \{0, 1\} \) and \( \sum_k M_{i,k} = 1, \forall i \). Furthermore, let \( \epsilon_{i,k}^{(q)} = \| \mathbf{x}_i^{(q)} - \mathbf{\mu}_k \| \) be the short-hand notation for the negative log-likelihood of object \( i \) from dataset \( q \) given cluster \( k \). As the full data likelihood factorizes, the cost function of GMM (with fixed covariance) is \( R = \sum_{i=1}^{n} \sum_{k=1}^{K} M_{i,k} \epsilon_{i,k}^{(q)} \). The hypothesis space for this centroid-based clustering model is parameterized by the cluster assignments. The transformations used in the coding scenario modify these clusterings. Therefore, we obtain the individual weight sums and the joint weight sum by summing over all possible clustering solutions

\[
Z_q = \sum_{c \in C(\mathbf{X}^{(q)})} \exp \left( -\beta \sum_{i=1}^{n} \sum_{k=1}^{K} M_{i,k} \epsilon_{i,k}^{(q)} \right) = \prod_{i=1}^{n} \prod_{k=1}^{K} \exp \left( -\beta \epsilon_{i,k}^{(q)} \right), \quad (9)
\]

\[
Z_{12} = \sum_{c \in C(\mathbf{X}^{(2)})} \exp \left( -\beta \sum_{i=1}^{n} \sum_{k=1}^{K} M_{i,k} (\epsilon_{i,k}^{(1)} + \epsilon_{i,k}^{(2)}) \right) = \prod_{i=1}^{n} \prod_{k=1}^{K} \exp \left( -\beta (\epsilon_{i,k}^{(1)} + \epsilon_{i,k}^{(2)}) \right). \quad (10)
\]

By substituting these weight sums to eq. 7, the mutual information amounts to

\[
I_\beta = \log K + \frac{1}{n} \sum_{i=1}^{n} \left( \log \sum_{k=1}^{K} e^{-\beta (\epsilon_{i,k}^{(1)} + \epsilon_{i,k}^{(2)})} - \log \sum_{k=1}^{K} e^{-\beta \epsilon_{i,k}^{(1)}} \sum_{k'=1}^{K} e^{-\beta \epsilon_{i,k'}^{(2)}} \right). \quad (11)
\]

The approximation capacity is numerically determined as the maximum of \( I_\beta \) over \( \beta \).
3.2. Experimental Evaluation

We define $K = 5$ Gaussians with parameters $\pi_k = 1/K$, $\mu = [(1, 0); (0, 1.5); (-2, 0); (0, -3); (4.25, -4)]$, and with covariance $\Sigma = 0.5 \cdot I$. Let $X^{(q)}$, $q \in \{1, 2\}$ be two datasets of identical size $n = 10,000$ drawn from these Gaussians. We optimize the assignment variables and the centroid parameters of our GMM model via annealed Gibbs sampling. Thereby, we provide double as many clusters to the model in order to enable overfitting. Starting from a high temperature, we successively cool down while optimizing the model parameters. In Figure 2(a), we illustrate the positions of the centroids with respect to the center of mass.

At high temperature, all centroids coincide, indicating that the optimizer favors one cluster. As we cool down, the centroids separate into increasingly many clusters until, finally, all 10 clusters are used to fit the data.

Figure 2(b) shows the numerical analysis of the mutual information (eq. 11). When the stopping temperature of the Gibbs sampler coincides with the temperature $\beta^{-1}$ that maximizes mutual information, we expect the best tradeoff between robustness and informativeness. And indeed, as illustrated in Figure 2(a), the correct model-order $\hat{K} = 5$ is found at this temperature. At lower stopping temperatures, the clusters split into many instable clusters which increases the decoding error, while at higher temperatures informativeness of the clustering solutions decreases.

**Relation to generalization ability:** A properly regularized clustering model explains not only the dataset at hand, but also new datasets from the same source. The inferred model parameters and assignment probabilities from the first dataset $X^{(1)}$ can be used to compute the costs for the second dataset $X^{(2)}$. The appropriate clustering model yields low costs on $X^{(2)}$, while very informative but unstable structures and also very stable but little informative structures have high costs due to overfitting and underfitting, respectively.

We measure this generalization ability by computing the “transfer costs” $R(c^{(1)}, X^{(2)})$: At each stopping temperature of the Gibbs sampler, we take the current parameters $\mu^{(1)}$ and assignment probabilities $P^{(1)}$ inferred from $X^{(1)}$ and transfer them to $X^{(2)}$. The assignment probabilities $P^{(1)}$ follow a Gibbs distribution

$$p(\mu_k^{(1)} | x_i^{(1)}) = Z_x^{-1} \exp \left( -\beta \| x_i^{(1)} - \mu_k^{(1)} \|_2^2 \right),$$

with $Z_x$ as the normalization constant. The expected transfer costs with respect to these probabilities are then

$$\langle R(c^{(1)}, X^{(2)}) \rangle = \sum_{i=1}^n \sum_{k=1}^K p(x_i^{(1)}, \mu_k^{(1)}) \| x_i^{(2)} - \mu_k^{(1)} \|_2^2 \approx \frac{1}{n} \sum_{n=1}^n \sum_{k=1}^K p(\mu_k^{(1)} | x_i^{(1)}) \| x_i^{(2)} - \mu_k^{(1)} \|_2^2,$$ (13)

Figure 2(b) illustrates the transfer costs as a function of $\beta$ and compares it with the approximation capacity. The optimal transfer costs are obtained at the stopping temperature that corresponds to the approximation capacity.

**Relation to BIC** Arguably the most popular criterion for model-order selection is BIC as proposed by Schwarz (1978). It is, like wASC, an asymptotic principle, i.e. for sufficiently
Figure 2: Annealed Gibbs sampling for GMM: Influence of the stopping temperature for annealed optimization on the mutual information, on the transfer costs and on the positions of the cluster centroids. The lowest transfer cost is achieved at the temperature with highest mutual information. This is the lowest temperature at which the correct number of clusters \( \hat{K} = 5 \) is found. The hierarchy in Fig. 2(a) is obtained by projecting the two-dimensional centroids at each stopping temperature to the optimal one-dimensional subspace using multidimensional scaling. BIC verifies correctness of \( \hat{K} = 5 \).

many observations, the fitted model preferred by BIC ideally corresponds to the candidate which is a posteriori most probable. However, the application of BIC is limited to models where one can determine the number of free parameters as here with GMM. Figure 2(c) confirms the consistency of wASC with BIC in finding the correct model order.

4. Conclusion

Model selection and model order selection pose critical design issues in all unsupervised learning tasks. The principle of maximum approximation capacity (wASC) offers a theoretically well-founded approach to answer these questions. We have motivated this principle and derived the general form of the capacity. As an example, we have studied the ap-
proximation capacity of Gaussian mixture models (GMM). Thereby, we have demonstrated that the choice of the optimal number of Gaussians based on the approximation capacity coincides with the configurations yielding optimal generalization ability. Weighted approximation set coding finds the true number of Gaussians used to generate the data.

Weighted approximation set coding is a very general model selection principle which is applicable to a broad class of pattern recognition problems (for SVD see Frank and Buhmann (2011)). We have shown how to use wASC for model selection and model order selection in clustering. Future work will address the generalization of wASC to discrete continuous optimization problems, such as sparse regression, and to algorithms without cost functions.

References


